Chips Volume XVI Issue II

Space & Naval Warfare Systems Command
Rear Admiral John A. Gauss

Naval Computer & Telecommunications
Area Master Station Atlantic
Commanding Officer
Captain N. Brown

Editor
Diane Hamblen
Assistant Editor
Elizabeth Dickason

Chips is published quarterly and is sponsored by Navy IT Umbrella Program Office, Space and Naval Warfare Systems Command, San Diego, CA.
Chips is produced on a Macintosh PowerPC running PageMaker 6.0.
Submissions. Articles and other contributions are welcome. We reserve the right to make editorial changes. All articles printed in ***Chips*** become the sole property of the publisher. Reprint authorization will be granted at the publisher's discretion.
Chips. Requests for distribution changes or for other assistance should be directed to ***Editor, Chips***, NCTAMS LANT, 9625 Moffett Ave, Norfolk, VA 23511-2784, or call (757) 444-8704; DSN 564. The e-mail address is chips@email.chips.navy.mil; FAX (757) 445-2103; DSN 565.
World Wide Web address is http://www.chips.navy.mil
Training. Phone Commercial (757) 444-7976; DSN 564

Disclaimer

The views and opinions contained in ***Chips*** are not necessarily those of the Department of Defense nor do they constitute endorsement or approval by the Naval Computer and Telecommunications Area Master Station LANT. The facts as presented in each article are verified insofar as possible, but the opinions are strictly those of the individual authors.

Chips is published quarterly by the Commanding Officer, Naval Computer and Telecommunications Area Master Station LANT, 9625 Moffett Ave., Norfolk, VA 23511-2784. USPS 757-910 Periodical postage paid at Norfolk, VA and at additional mailing office. POSTMASTER: Send changes to ***Chips***, NCTAMS LANT.

Cover Story

Features

Editorial

The party's over; let's call it a day. The old song from the 40s says it all. It is over; this is my last editorial. I hoped when this day came I'd have something profound to say. I don't. But, as I look back on 47 editions of ***Chips***, I can rest easy because I tried to serve not just the Navy but all of DoD. In the final analysis that's what counts.

Editorials have been the most difficult part of my job. Probably because I have an opinion on almost everything, and it rarely matches the opinion I'm supposed to have. The checks and balances were sometimes more check than balance, as I pushed everyone's patience to the limit. It was a game of sorts for me, one that exercised my brain and, hopefully, made others think as well.

I'm proud that my very first interview in July 1986 with RADM Grace Hopper is as fresh today as it was then. Hopper's predictions were and are accurate. I'm grateful I didn't let her down. I think she would have kept her promise to come back and haunt me if anything had happened to ***Chips*** on my watch.

Chips has established a few pretty important firsts. ***Chips On-Line*** was the first electronic magazine in existence. The first issue was mailed in January 1987 over the old DDN. We were the first government magazine on the world wide web. The first issue for that was July 1995. I'm relatively sure that we're the first (and probably the only) government magazine to have a readership in excess of half a million.

I've interviewed some powerful people over the years – Admirals, Generals, DoD's senior civilians, important project managers. I was never at a loss for questions because I'm so hopelessly nosey. I'd always wondered if that was a bug or a feature, and it was Hopper who made me comfortable with it. During our first interview she asked me to name the one thing that I felt qualified me to be the editor of ***Chips***. I didn't think she cared about my resume, so I answered, "I'm inquisitive." Her reply? "That will do."

But, ***Chips*** never belonged to me. I was only the caretaker. Everyone who contributes articles and answers my never ending questions make up the real ***Chips***. Elizabeth Dickason, the ***Chips*** assistant editor, and I fought, made up and fought some more, the way good team mates do. I owe her more than I can ever say. David Rook, my husband, and NCTAMS LANT's senior computer scientist spent untold hours trying to explain concepts that were over my head. The most memorable of which was the feature article on Copernicus when I must have set a record for saying, "But, I don't understand.... What if...." And Jim Stakes who has been my department head for over 10 years who had faith, patience and above all a sense of humor.

Most of the memories are good but they are, after all, just memories. Now it's time to look towards the future. Will ***Chips*** change?

Yes. Absolutely, yes. A new editor will have different solutions to old problems. The tone, content, attitude and the very essence of ***Chips*** will be different. But, hopefully, with change comes growth.

I think you can expect some emphasis shifts when it comes to content. What I thought was important may not be what the new editor thinks of as important. For me, the charm of this job was that I was allowed to follow my gut instincts. I could, within reason, decide what to write about, who to interview and what articles to accept from the outside world. It was a lot of responsibility, but fun. I wouldn't have missed it for the world. There aren't too many government jobs that are as challenging, stimulating and fulfilling as being the editor of ***Chips***.

My successor is Ernest Smith. He has had a long and varied government career which will serve as a cushion for the surprises that are in store for him. Treat him as you treated me. He can handle it.

Diane Hamblen

April Hot Spots

The drive to attain network-centric warfare capability has profound implications for security and requires a significant shift in the protection strategy. *Read about it beginning on page 4.*

Read Logistics Support for Legacy Systems if you have problems keeping older, but still valuable, systems online. Equipment supported includes certain computers, displays and peripherals. *See page 10.*

The Naval Vessel Register is the official inventory of ships and service craft in the custody of, or titled by, the U.S. Navy. It's now available online. *See page 18.*

ERM 101 teaches you the basics about electronic records management with Zippy as your guide.
See page 24.

Introducing the Chips Choice Web Site Review - spotlighting a .mil web site that provides well-presented, useful information with the right amount of style. *To see who we selected, turn to page 29.*

Defense in Depth: Security for Network-Centric Warfare

By CAPT Dan Galik, USN

On Friday, February 13, 1998 a Defense Information and Electronics Report was released which stated that a "widespread and potentially harmful attack" on seven Air Force and four Navy information technology (IT) sites had been detected. As of this writing, the attacks are still under investigation to determine their source and the full extent of their effects. The article indicated that the focus of most of the attacks was domain name servers (DNSs) which provide name/address translation for internetworked systems. While it appears that the attacks targeted only unclassified systems, the report serves as yet another demonstration that networked IT systems are vulnerable to attacks and need to be protected.

The news media are replete with reports of attacks on and via the Internet and the increasingly widespread Web, and book upon book has been written describing the details of known vulnerabilities and how they can be countered. Traditionally, the military has ensured the security of its information systems by a risk avoidance strategy: keeping its network infrastructure separate from the public Internet, and strictly limiting access to it via locked spaces, security clearances and cryptographic devices. However, the drive to attain network-centric warfare capability has profound implications for security and requires a significant shift in the protection strategy.

Network-Centric Warfare is Technology Based

The value of network-centric warfare has been clearly identified and discussed, and it enables the achievement of information superiority. The IT-21 initiative has been designed to achieve this information superiority in a time of limited resources and rapidly changing technology by requiring that the military capitalize on available commercial technology as much as possible. *IT-21 is a transformation in the C4ISR warfighting process that focuses on:*

- Movement away from expensive, single-function workstations to affordable, highly-capable personal computers.
- Extensive use of web technology to manage data to produce knowledge.
- Seamless ashore/afloat transfer of voice, video and data information.
- TCP/IP-based, client-server environment with multi-level security.
- Embracing of industry standards, open architectures and COTS.
- Merging of tactical and non-tactical data on a common infrastructure.

The IT-21 initiative leads to the adoption of open standards (DII-COE) and commercial off-the-shelf (COTS) technology (Windows NT). Additionally, it leads to migration away from separately developed and connected *stovepipe systems* which cannot interoperate or communicate, to fully integrated and interoperable systems connected via a common infrastructure. While much of this common infrastructure is separate from the public Internet, it is important to note that the unclassified military network currently includes multiple connections to the Internet, and that the plan is to migrate toward a common infrastructure to be shared by both unclassified and classified networks.

The Naval Virtual Intranet (NVI) concept works as part of the IT-21 Initiative to further develop the goal of speed of command via information superiority. NVI seeks to capitalize on the common infrastructure and interoperability of systems to achieve efficiencies of information processing by centralizing information services as much as possible in a limited number of data processing centers, the Regional Information Technology Service Centers (RITSC).

The combination of open standards, COTS technology, full connectivity and information service regionalization compels us to develop a new protection strategy based not on risk avoidance, but rather on risk management. No longer can we rely on limiting access to one-of-a-kind custom-developed systems with limited connectivity. We are now embracing widely-known common technologies, recognizing that some of the these technologies come with well-documented vulnerabilities. Further, as more and more systems are interconnected, the user population increases significantly, thus increasing the threat of *insider attacks.* Finally, regardless of the level of insider threats, the sharing of a common infrastructure which connects with the public Internet brings with it a world-wide host of hackers, criminals and foreign agents who are practiced and capable of surfing their way through that infrastructure.

Network-Centric Warfare is Information Intensive

Traditionally, security has focused on ensuring confidentiality: the non-disclosure of classified information to those who are not authorized to see it. While this remains an important consideration, the shift to network-centric warfare, with its goal of speed of command, is heavily reliant on both the accuracy and timeliness of information, and on the continued availability of critical communications channels. No military maneuver can succeed if its participants cannot communicate, or if their decisions and actions are based on inaccurate, bogus or outdated information. Many of the best known and most common attacks that occur on the Internet are those which target information integrity (such as viruses) or seek to bring down a system (such as flooding attacks). Some attacks, such as IP address spoofing, focus on masquerading which can result in planting bogus information. Other attacks such as corrupting the translation tables of a Domain Name Server can cut off or hijack communication channels. Thus, our protection strategy must address not only confidentiality, but also the integrity, authenticity and timeliness of information, and continued availability of processing and communications capabilities.

Perfect Security Cannot Be Achieved

The combination of open standards, COTS technology, and full connectivity on which network-centric warfare depends, requires that we focus priority attention on defining a strategy to counter a myriad of potential flaws and vulnerabilities. The flaws and vulnerabilities in the family of UNIX operating systems are well known and easily exploited, and we must continue to strive to plug up those holes in our systems that may continue to rely on UNIX. However, even intentionally designing security into a system (such as has been done with the Windows NT operating system) is no guarantee of success; the complexity of today's systems, coupled with the sometimes unexpected behaviors which result when two independently developed systems are connected, results in a never-ending, constantly changing list of flaws and vulnerabilities. Even systems which have been *hardened* by years of identifying and patching flaws continue to contain flaws and vulnerabilities that can be exploited by enterprising and resourceful hackers. It is this fact which necessitates the shift from a risk avoidance strategy to a risk management strategy.

While perfect security is a myth that cannot be achieved, there is much that can be done within the limits of the current state-of-the-practice to minimize system vulnerabilities and counter potential threats. To this end, the Navy has defined, as an integral part of the IT-21 initiative and the NVI, a Defense in Depth strategy which utilizes currently available protection technology in a layered system of defenses designed to protect the confidentiality, integrity, authenticity and availability of the information and IT systems on which network centric warfare depends. Table 1 below identifies currently available protection tools, and indicates which security requirements are typically targeted by each tool.

Protection Tool	Confidentiality	Integrity	Authenticity	Availability
Firewalls	yes		sometimes	sometimes
Encryption	yes	yes	yes	
Content checking		yes		yes
Source authentication		yes	yes	
Intrusion detection	yes		yes	yes
Access control	yes		yes	
Secure protocols	yes	yes	yes	
Audit	yes	yes	yes	yes

Table 1: Security requirements addressed by available protection tools

Firewalls. A firewall is an application layer gateway that is used to selectively allow external users access to information located behind the firewall. Also known as a bastion host firewall, it is installed between an information system or enclave network and an *outside*, usually public, network. Users within the protected domain can access the outside network via the firewall. In addition to providing a mechanism for implementing network access control, a properly configured and managed firewall can provide network intrusion prevention. To minimize costs and management overhead, a firewall may be installed in a central location, such as a Regional Information Technology Service Center (RITSC) and shared by multiple DoN systems connected via a secure intranet. The most widely used firewall for the Navy is the TIS Gauntlet.

Encryption: Encryption can be used to provide not only information confidentiality but also integrity and mutual authentication of the communicating parties. Appropriate use of encryption technology can provide cryptographic separation of information at different levels of classification, permitting such information to be communicated via a common infrastructure, and even *tunneled* across a non-secure public internet. The National Security Agency (NSA) evaluates the strength of cryptographic devices for securing classified data. NSA endorsed Type 1 devices are currently available to provide link layer, IP and ATM layer encryption. Currently, only one device is available for IP layer encryption, the Network Encryption System (NES), and one device for the ATM layer, the Fastlane.

In FY99, NSA expects to release and endorse the Taclane, which will provide both IP and ATM encryption capability. This device will not interoperate with the NES and will not support Fast Ethernet, but will interoperate with the Fastlane at DS-3 rates. For unclassified information, a variety of software and hardware products are available which provide encryption and digital signature capabilities. The most commonly used standards include the Data Encryption Standard (DES) and a variation called 3DES (triple DES) for providing confidentiality, and Secure Hash Algorithm 1 (SHA-1) for providing data integrity and authentication.

Content Checking: Many forms of electronic information can contain harmful content such as viruses, worms and Trojan horses. These *malicious programs* can be transmitted across a network in a number of ways including SMTP e-mail attachments, FTP file downloads, and Java applets. Numerous COTS products exist that can check these routes to identify such potentially harmful content, and two of these products, Norton and McAfee, are available on the DoD-wide virus-detection tool site license (see http://infosec.navy.mil). If properly configured and frequently updated, these tools can identify harmful content before it has the chance to do any damage, and in many cases can repair already damaged files. Content checking is often done as part of a firewall in addition to being done on the end-user workstations.

Source Authentication: Certain network components, such as routers and Domain Name Servers, maintain tables (routing tables, name/address translation tables) which are critical to their correct functioning, and which are updated regularly by their peers within the network. Without authentication of the source of the updates, it is easy to spoof the information, resulting in denial of service or network intrusion. Many COTS IP routers feature cryptographic authentication of updates for selected routing protocols. These features can often be utilized by simply reconfiguring existing routers. Currently, the BGP and OSPF routing protocols support cryptographic authentication.

Intrusion detection: Network intrusion filters (NIF) may be less restrictive than firewalls and thereby allow a wider range of network applications to be used while still being able to detect and block a wide variety of network attacks. Several vendors are currently producing NIF products, including stateful filtering routers and active, real-time intrusion detection systems. Stateful filtering routers are similar to normal filtering IP routers, and can be used to allow or disallow incoming packets based on source/destination IP addresses and TCP ports. In addition, stateful routers use knowledge of higher layer protocols to identify and allow legitimate protocols and to identify and disallow certain network attacks.

Active intrusion detection systems (IDS) also use knowledge of higher layer protocols to identify network attacks. When an attack is detected, it can be reported, often in real time, to a central monitoring facility and possibly blocked (e.g., using a TCP connection reset). Depending on its configuration, an active IDS may be able to provide a high level of security in a non-intrusive manner. The Fleet Information Warfare Center (FIWC) is the key organization that serves as the Navy's central reporting point for all information system incidents.

Access control: In addition to the access controls that can be provided by firewalls, filtering routers and intrusion detection systems, individual end systems such as user workstations and data or application servers usually provide access control mechanisms. These include user IDs and passwords, and file access control lists which can be very effective in limiting access to the information that

►

resides there. These same mechanisms, however, if not configured and administered properly, can be significant vulnerabilities. For example, many systems have well-known default guest accounts and/or default passwords.

Secure protocols: Protection of unclassified information in transit and assembly of protected communities of interest are becoming possible via the use of network protocols that encrypt information and provide information integrity. Currently the two most attractive protocols are the Secure Sockets Layer (SSL) and the Internet Protocol security suite (IPsec). SSL is typically used to protect communications between a web server and a web browser. The IPsec protocol is used to build encrypted virtual private networks (VPNs) between groups of users.

Auditing: While auditing itself cannot prevent any security violations, it can be very useful in establishing and documenting the source of a violation, and assessing the extent and nature of the damage sustained. Audit trails may be used as input for intrusion detection systems, and can usually be *tuned* to avoid resource exhaustion by specifying what events are to be audited.

Putting It All Together

The security tools described in this article are all part of the currently available COTS technology and are being employed to enhance the security of the Navy's information infrastructure. While no single tool provides complete security, a well-planned deployment of multiple tools that complement and reinforce each other can significantly strengthen and harden that infrastructure. This is the goal of the Navy's Defense in Depth strategy. *The protection requirements of the NVI include:*

- Service via a protected network infrastructure all the way to each subscriber's facility (protected, *hardened* routers, ATM switches, DNS services).
- Securely configurable operating systems on all servers and clients.
- Secure protocols (authentication, integrity and confidentiality) for all client-server and server-server interactions (http, messaging, network news, FTP, etc.).
- Firewalls at processing and/or subscriber facilities (including malicious connection/content screening).
- Intrusion detection devices on LANs.
- On-line virus protection.
- Active security and configuration monitoring of the infrastructure.

The Defense in Depth strategy for IT-21/NVI addresses these protection requirements by employing security protection mechanisms in layers at multiple locations in the system architecture. The intent is to provide a combination of protection mechanisms that is broad enough to address all the security requirements and deep enough to provide redundancy across multiple layers. For example, within encryption, depth may mean combining link encryption under network (IP layer) encryption under email (application layer) encryption. Another example would be to use two different antiviral packages (perhaps one on a firewall and another on the end-user workstations) so that if a virus is undetected by one package, it may be caught by the other. This approach ensures DON systems maximize resistance to attacks and minimize the probability of a security breach due to a weakness in any single security mechanism.

The Defense in Depth strategy is directly analogous to sea control concepts. Fleet air defense can serve as an example. An outer defense zone is defended by intercept fighters such as F-14s and controlled by E-2Cs. A second layer of defense is the missile zone defended by Aegis cruisers which intercept attackers that have not been stopped by the outer layer. Inside the missile zone lie the point defense zones where the defensive weapons are chaff, close in warfare systems and tactical electronic warfare machinery. If the system is working properly, the number of attacks that penetrate to the inner zone is less than the capacity of the point defense weapons.

The generic framework for Defense in Depth is illustrated in Figure 1 below. Four zones of defense are defined in this framework. These zones may be logical and are not necessarily physically separate. The selection, placement and configuration of particular security mechanisms are implementation dependent and are driven by the information protection requirements for the particular DoN information system that is being protected.

Zone 4: The outermost zone represents the boundary between a DON information system (or multiple DON information systems connected by a private intranet) and a public internetwork such as NIPRNET or SIPRNET. Defenses that are most appropriate here include firewalls, Virtual Private Network (VPN) encryption, content checking, and source authentication for routers and DNSs.

Zone 3: This zone delineates a Community of Interest (COI). The protections that are deployed here are designed to provide protection within and between such COIs. In general, Zone 3 information protection mechanisms are installed as part of an intranet used to connect end user networks that have similar security requirements and a common COI. Zone 3 information protection mechanisms may include network intrusion filters, firewalls, VPN encryption and content checking.

Zone 2: A single COI may include a number of individual sites or enclaves, each of which represents a layer 2 zone. Security mechanisms deployed here are used to provide protection at the boundary to the site or enclave and are generally integrated as part of the site/enclave LAN. Zone 2 information protection mechanisms may include network access controllers, network intrusion filters, firewalls, VPN encryption, and content checking.

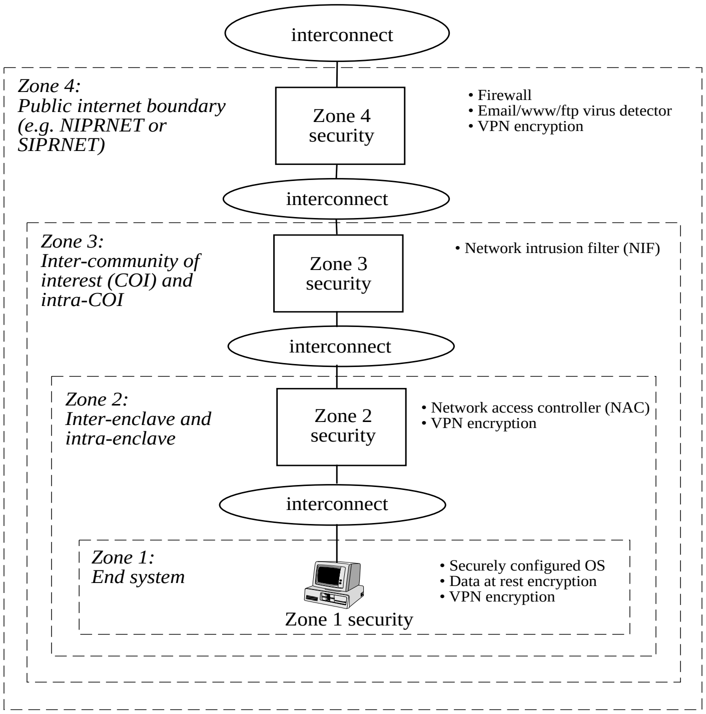


Figure 1: Defense in Depth Framework

Zone 1: The innermost zone is the individual end system and includes components such as workstations, servers (NT and/or UNIX) and mainframes. The operating systems must be deployed with all known holes and weaknesses fixed (as practical). The Navy and the National Security Agency (NSA) have both published secure configuration guides for Windows NT, and these guides are being used by our system developers. Zone 1 information protection mechanisms provide the innermost layer of defense for DoN systems, and may include the following: system access controls such as passwords, data access controls such as Access Control Lists (ACLs), encryption of data/files, email and web transactions, VPN encryption, content checking, auditing and careful design of user applications.

If properly designed, carefully deployed, and regularly maintained, the Defense in Depth strategy can significantly enhance the security posture of the Navy's information infrastructure, to ensure that the information it provides to the warfighter is properly protected, accurate, and timely, and that the data and communications channels essential to command are instantly and always accessible. Such protections play a critical role in establishing and maintaining the Navy's information superiority and effecting the speed of command that is vital to our warfighting capability.

More detailed information describing the Defense in Depth strategy, protection mechanisms and current policy and standards can be found at the Navy INFOSEC web page (http://infosec.navy.mil). The Navy INFOSEC Program Office (SPAWAR PMW 161) maintains this web page, with comprehensive links to INFOSEC information, including information on available security products, links to anti-viral tools, INFOSEC news and articles, security policies and procedures, and links to the Naval Computer Incident Response Team (NAVCIRT).

In addition, FIWC is the information warfare center of excellence for the Navy and the owner of NAVCIRT. FIWC publishes NAVCIRT advisories, alerting the Fleet to viruses and vulnerabilities in common computer networks or systems. Another significant support service available from FIWC includes the Vulnerability Analysis and Assessment Program (VAAP), which includes conducting On-Line Surveys (OLS), to test for vulnerabilities of fielded/legacy networked systems. FIWC also supports red team operations, which have a main goal of increasing security awareness, and to train system administrators in incident recognition. All of these services contribute to the Defense in Depth strategy. To contact FIWC, send an email to navcirt@fiwc.navy.mil.

References:

Network-Centric Warfare - Its Origin and Future, by Vice Admiral Arthur K. Cebrowski, USN, and John H. Garstka. *Proceedings of the U.S. Naval Institute*, Vol 124/1/1,139 January 1998.

IT-21 Intranet Provides Big "Reachbacks" by Rear Admiral Robert M. Nutwell, USN. *Proceedings of the U.S. Naval Institute*, Vol. 124/1/1,139 January 1998.

About the Author: CAPT Galik is the head of the Navy INFOSEC Program Office (SPAWAR PMW 161). His e-mail address is galikd@spawar.navy.mil.

Connecting Technology Spring '98
Norfolk Waterside Marriott
May 12-14, 1998

• See the back cover for more details. •

First Name ______________________ Middle Initial ______

Last Name ______________________________________

Job Title ______________________________________

Organization Type (See box at right for choices) ______________

Agency/Command (Address Line 1) ____________________

Address Line 2 __________________________________

Address Line 3 __________________________________

Organization Type

- Navy
- Air Force
- Army
- Marines
- Coast Guard
- Government (non-DoD)
- Government Contractor
- Other Contractor/Vendor
- Not Listed

City ________________ State/Country ________________ Zip Code __________

Commercial Phone Number ______________________________

DSN Number ______________________________________

Fax Number ______________________________________

Email Address ____________________________________

Mail to: Bobbi Drexler • NCTAMS LANT • 9625 Moffett Ave • Norfolk, VA 23511-2784 • Fax (757) 445-2103; DSN 565

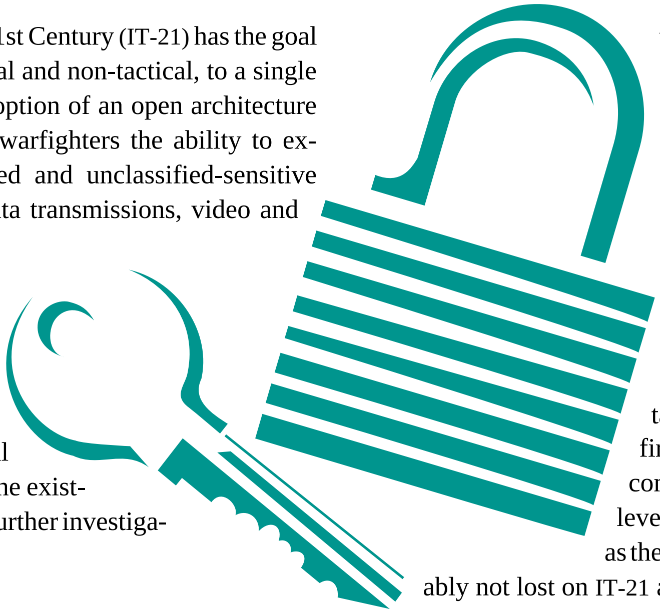
The Security Implication of IT-21

By Chris McDonald

Information Technology for the 21st Century (IT-21) has the goal to drive all applications, both tactical and non-tactical, to a single desktop PC. IT-21 proposes the adoption of an open architecture with multi-level security to allow warfighters the ability to exchange information that's classified and unclassified-sensitive through a network that includes data transmissions, video and voice.

This is not only an ambitious enterprise, but also one which challenges all Navy personnel.

This article will examine potential IT-21 security implications against the existing record, and suggest avenues for further investigation.



> "Security used to be an inconvenience sometimes, but now it is a necessity all the time."
> *– Martina Navratilova remarked after the stabbing of Monica Seles by a fan of Steffi Graf, 1993*

The same quote is applicable to information systems security. Clearly IT-21 architects have planned for security. Still one can examine their planning process from the perspective of a variation of Murphy's Law: "If anything can go wrong, it will and at the worst possible moment."

The architects have selected Microsoft's Windows NT 4.0/5.0 as the centerpiece. What do we know about this operating system? First, NT 4.0 does not have evaluation as a trusted operating system under the National Computer Security Center's (NCSC) Trusted Computer System Evaluation Criteria or Orange Book. NCSC did assign a C-2 level to a standalone 3.5 version of the operating system, one in which there was no network access to the system, where floppy disk drives had been removed or disabled and where access to the standard file system had been intentionally made more restrictive. Clearly IT-21 could not exist under that model.

Second, unlike the UNIX operating system, for which we have almost 30 years of experience, NT has been in existence for only 10 years and is less mature. We have seen several events to suggest NT's *youth* may present some security implications. On July 4, 1997, the Russian developer Konstantin Sobolev released a utility on the Internet that allowed any user on a Windows NT computer to be added to the administrators group.

This *getadmin* utility used a bug in the Windows NT kernel to change the value of an internal system flag which governs whether security checking is performed on certain accesses to processes. This was the first publicized NT exploit in which a common user could elevate permission levels. The significance of the date as well as the nationality of the developer was probably not lost on IT-21 architects.

While the exploit itself was a major Internet event, the Microsoft response was equally newsworthy. Within days of Microsoft's release of a hotfix, another researcher, Constin Raiu, had posted additional exploit code which permitted getadmin to still function. In this instance, Raiu's Internet electronic address and Web site were in a foreign domain. This only continued the international flavor of exploit mania.

The exploit and subsequent publicity on the flawed hotfix highlight a major problem for IT-21 architects: namely, how robust is the Microsoft security development, testing and response procedure? The USENIX association, normally the bastion of UNIX system administrators, had a Windows NT Security panel at its last major conference in 1997. The panel, moderated by Mike Masterson of Taos Mountain Software, consisted of Bridget Allison of Network Appliances, Jeremy Allison of Whistle Communications (SAMBA), Peter Kochs of Digitivity, and Peter Brundrett, a Microsoft program manager. The summary of that panel, published in the November 1997 edition of *;login:* offers some ideas on the question.

Mr. Allison noted that the system call interface to NT is undocumented, an issue mentioned even by Microsoft employees. The reason is that the NT kernel changes faster than documentation can keep up. Essentially, the source, some 16-20 million lines of code, is the documentation (18 CD-ROMs). Mr. Brundrett from Microsoft responded by noting that there are some 2,600 system service APIs in NT versus 157 system calls in the 4.4BSD Unix. He then confirmed that there are security APIs that have not been documented.

Mr. Brundrett admitted that Microsoft, unlike Sun, IBM, SGI and other vendors, had not worked directly with the Forum of Incident Response Teams (FIRST) or the Computer Emergency Response Team at Carnegie Mellon (CERT/CC). While he promised *to look into* such participation, IT-21 architects still face the prospect of a vendor which as yet does not actively participate in a major security initiative.

A representative from CERT/CC asked Mr. Brundrett if Microsoft has procedures to validate and verify the NT kernel. Though the Microsoft representative stated that his company has tools to do this, there was not a follow-up question to inquire whether testing should have revealed the getadmin problem prior to its discussion on the Internet.

If we assume that IT-21 architects have worked their way through the above issues, then why not throw in three additional items for the sake of emphasizing Caveat Emptor (Let the buyer beware)? First, there is agreement that existing Windows NT security default permissions on shares, registry settings and system permissions are inadequate. Second, the interoperability of several application products with the Windows NT operating system can sometimes result in unexpected exposures. Known vulnerabilities and exploits for Internet Explorer, Power Point and FrontPage 97 have all facilitated attacks against NT servers.

If I were an IT-21 architect, what would my plan of action be at this point? Clearly the user community has to understand how multi-level security will be obtained when the operating system is not certified for multi-level operations. Delivery and installation of planned hardware and software must proceed with documented, uniform NT configuration policies and procedures. System administrators must know in advance the appropriate and necessary security permissions on shares, registry settings and system file permissions. They must have a clear idea of how to establish trust relationships between domains; what user, system and audit policies to establish; and the necessity to regularly check ownerships, group memberships, access permissions and rights and abilities.

IT-21 architects must have a direct, documented relationship with Microsoft so that critical information related to potential security exposures can be obtained and shared first within the Navy community. Proprietary and secrecy agreements are not new. NCSC in its evaluation of products against the Orange Book criteria established the baseline for such agreements with private industry many years ago.

IT-21 architects must provide system administrators with automated tools to assist them in monitoring their implementation of NT security policies and procedures. The Department of Energy has released a Security Profile Inspector (SPI) for Windows NT that may be used within the DoE and DoD communities. However, the tool is new and is not presently as robust as a commercial tool, the Kane Security Analyst (KSA). The distribution of SPI and the judicious site-licensing of KSA may be key elements in the secure maintenance of IT-21 assets.

IT-21 architects must assume that attacks against Windows NT and its bundled applications will increase, and must, therefore, concentrate on those strategies which will most effectively manage, if not reduce, the potential for disaster. This may include policy instructions on what network services will be run, what applications to permit or disable, and what ports or services to block or filter at the router or firewall level. It may involve verification procedures to distribute secure hotfixes, and in some cases to ensure the adequacy of a hotfix prior to distribution throughout the Fleet. It may require augmentation to existing intelligence and counterintelligence resources to monitor the Internet for potential attack programs and scenarios of attack.

Finally, IT-architects must adopt some humility and a sense of perspective on the task they and their users face.

> *Nathaniel Borenstein has written:* "The most likely way for the world to be destroyed, most experts agree, is by accident. That's where we come in; we're computer professionals. We cause accidents." The technical challenges and complexity of IT-21 is more than just the sum of its individual components.

About the Author: McDonald is the Information Systems Security Manager for White Sands Missile Range, NM, and is a certified information systems security professional (CISSP). His e-mail address is mcdonalc@wsmr.army.mil.

Logistics Support for Legacy Systems:
Tactical Embedded Computer Resource Reutilization

By Don Petkus

Introduction. Do you have problems keeping older, but still valuable, systems on-line? Anyone who has tried to keep their favorite old car running knows how hard it can be to get parts. Similar problems face system operators and maintainers in the fleet.

The Navy has highly capable systems, but the difficulty and time needed to get ready-for-issue (RFI) assets affects availability. While the future of the Navy's computer resources may well lie in off-the-shelf acquisitions and the integration of tactical and non-tactical applications, the fleet will require support for specific applications into the next millennium. (See "IT-21 - Moving to the 3rd Stage," *U.S. Naval Institute Proceedings*, May, 1997 and "IT-21: The Path to Information Superiority," *Chips*, July, 1997. Both articles were written by Admiral Archie Clemins, Commander in Chief U.S. Pacific Fleet.)

Tactical Embedded Computer Resources (TECR) are standard computers, peripherals and displays that serve as equipment or subsystems in communications, cryptology and weapons systems. For example, the Naval Modular Automated Communications System (NAVMACS) relies upon embedded AN/UYK-7 and AN/UYK-20 computers, AN/USH-26 cartridge tape systems, AN/USQ-69 data terminal sets and OL-267 input/output data displays. Until NAVMACS installations are completely replaced by NAVMACS II, the older system will require support for its embedded legacy equipment.

Many other major systems incorporating TECR are in a similar position. Figure 1 depicts a generic weapon system that is TECR reliant. Specific TECR in any system depends upon the system configuration and variant.

Support at the End of a Life Cycle. Because TECR items are in late or post-production, piece parts, modules and end items to repair or replace these products are often hard to acquire. Fortunately, a reutilization program mandated by the Assistant Secretary of the Navy (Research, Development and Acquisition) and managed by Naval Sea Systems Command (NAVSEA) is on-line to support the reutilization program for standard embedded computer resources. This program is available to the Navy, Marine Corps, Coast Guard, other armed forces and foreign military sales customers.

Program Function. The NAVSEA TECR reutilization program supplies end-item assemblies, subassemblies/modules, line replaceable units and piece parts. These items can have supply COG codes of 1H-9N. Assets become available for reutilization when the original program office declares them as excess, often as a result of a ship decommissioning. After recovery, these assets are inspected, tested, repaired, refurbished and returned to RFI condition.

The cost of inspecting, testing, refurbishing and certifying assets as RFI is passed on to the customer. If there is no asset in the inventory with the necessary configuration to meet a specific customer's needs, an available asset can be reconfigured. Upgrades and reconfigurations are, of course, based on the assets available in the reutilization pool.

Under the management of SEA 91W, the TECR reutilization program maintains a facility at Naval Surface Warfare Center's Crane Division. The reutilization facility is co-located with an ISO 9002 certified organic depot and certain TECR program management functions. The co-location of these functions and assets has proven useful in supporting casualty reports (CASREPs), reverse engineering, life extension and other areas.

TECR assets are reutilized to support the following functions:

- Overhaul/restoration support
- CASREP support
- Naval Inventory Control Point support
- Depot support
- Supplementing new procurement

Products & Services. Products available through the program range from modules to entire end items. Services include certifying assets as RFI, refurbishment as needed, shipping and handling. In some instances, refurbishment and re-configuration are necessary to bring an item in the inventory up to customer expectations and requirements. Since the reutilization facility is co-located with program management, a wide spectrum of program and logistics support is available including contract access, technical manuals and other data.

The equipment supported is categorized as computers, displays and peripherals. They include such classics as the still widely used AN/UYK-7(V). The major equipment supported is listed at the right.

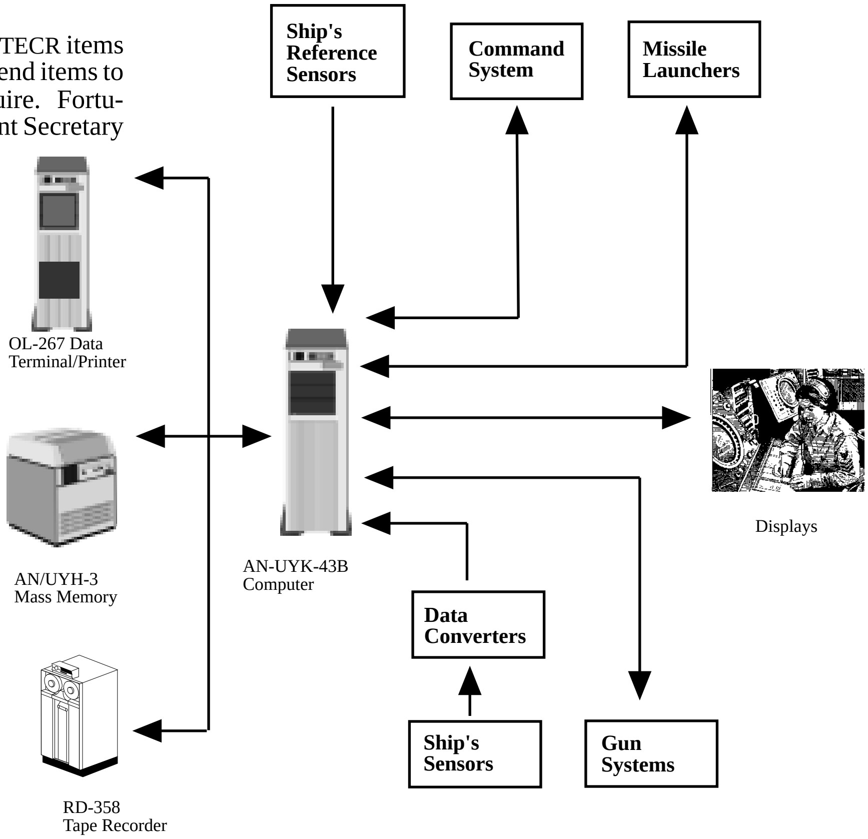


Figure 1: Typical Combat System with Legacy Embedded Computer Resources

Computers	AN/UYK-7 embedded mainframe
	AN/UYK-20 embedded mini
	AN/UYK-43 embedded mainframe
	AN/UYK-44 embedded mini
Displays	AN/UYA-4 data display group
	AN/UYQ-21 computer display system
	OL-267(V) input/output console/display unit
	AN/USQ-69 data terminal set
Peripherals	AN/UYH-3 magnetic disk set
	RD-358 magnetic tape recorder
	RD-358 Amagnetic tape recorder
	OJ-172 data exchange auxiliary console
	AN/USH-26 cartridge tape system

Partial support for some orphans not listed here has been established. Interested parties should feel free to communicate with the points of contact identified in this article.

TECR Supported Systems. TECR-reliant systems are aboard various naval, military and FMS weapon platforms. A few of the major systems that can benefit from the reutilization program include:

NAVMACS
TRIDENT
AEGIS
CDS/ACDS
AN/SQQ-89
NTDS
SURTASS
AN/BQQ-5E
SATIR
AN/BSY-1
Vertical Launch Systems (VLS)
MK 68/86/92 Fire Control Systems
MK 116 Underwater Fire Control System

Who Are Our Customers? The ultimate customer is the end-user in the fleet or other operating forces. In general, combat systems offices; supply and maintenance personnel; port engineers; supervisors of shipbuilding, conversion and repair; CASREP process people; and OEMs can benefit from the program. Although program management for the reutilization program resides in NAVSEA, the products and services are available not only Navy-wide, but to any authorized stakeholder in the equipment, including contractors.

Private Sector Access. Original equipment manufacturers (OEMs) and other government contractors can access TECR reutilization assets if they have appropriate tasking from the government. In the past, the assets have become available through two distinct paths: Government customers, such as combat system managers, have received material from the program which later became government furnished material or equipment. In other cases, contractors have been able to get modules or end items from the reutilization program to fulfill their government tasking.

On occasion, some of these assets were originally produced by the OEM who no longer has the production capability or inventory of some of these mature technologies.

Frequently Asked Questions

Potential program users frequently have similar questions. A few are listed below. For more information, consult the points of contact and the TECR web page listed at the end of this article.

Question: *What use is the program to the current owners of excess TECR, especially if they plan on replacing their assets with COTS? If they have excess TECR, they certainly don't need more.*

Answer: The program can be useful to TECR owners since excess material can be transferred **to** the reutilization program. This avoids the cost of providing sheltered storage for these bulky items. The AN/UYK-43(V) computer, for instance, is the size of a refrigerator. Transferring custody of refrigerator-sized assets frees up space and makes the asset available elsewhere.

Question: *Do I have to buy an entire end item in order to cannibalize a circuit card assembly or similar module?*

Answer: The reutilization facility can remove, certify and ship as RFI such items, provided they are in stock.

Question: *Does this program operate outside the established supply system?*

Answer: We're not a clandestine supply operation. The reutilization program operates in coordination with the Naval Supply Systems Command and the cognizant item managers.

The program works with the supply system to save time and money. For example, in support of a Federal German Navy FMS case, a $500K cost avoidance was realized through the use of the supply system rather than buying parts direct from the OEM.

In another Federal German Navy case, twelve months were saved in upgrading AN/UYK-20 computers by using reutilized assets from decommissionings.

Question: *Why use this program when COTS replacements are the obvious solution to late and post-production problems?*

Answer: Many programs don't have the funding to retrofit their systems with COTS replacements.

Sometimes a source of repair parts or a rotatable pool of assets is a practical solution. Bringing a system on-line that only needs to last until its next generation replacement can be cheaper than an interim engineering fix. A technology insertion can add years to the useful life of a TECR reliant system.

In the case of the MK 86 Fire Control System, a successful life-extension program used assets from the AN/UYK-7(V) reutilization inventory combined with new software and a semiconductor memory replacement to produce the Enhanced Memory Unit (EMU). This approach resulted in a $15M cost avoidance for the program office and satisfied the system's expanded requirements.

Question: *Why aren't assets free to authorized users since the government has already paid for them?*

Answer: Most customer costs spring from refurbishment, reconfiguration, testing and certification of assets originally received as non-RFI. Generally, assets in the inventory must be certified as RFI before they can be released to meet customer requirements.

Need More Information? Contact Gary Whittacre at SEA 91WP3 for program information. He can be reached at (703) 602-1055; DSN 332, extension 219. The fax number is (703) 602-2070. E-mail: whittacre_l_gary@hq.navsea.navy.mil

Technical information and free estimates are available through Cliff Burk at the Crane Division. His telephone number is (812) 854-5534; DSN 482. The fax number is (812) 854-1547. E-mail: burk_cliff@crane.navy.mil

Visit the TECR program/reutilization web site at http://www.m42.crane.navy.mil/706/7063. Click on *Reutilization* for the latest information.

About the Author: Petkus works at the Naval Surface Warfare Center in Crane, Indiana. He can be reached via email at DAP@smtp.crane.navy.mil.

A Case for Laptops

By LT Paul Brotze, USN

During a typical work-up cycle, the average sea-going squadron is required to detach or deploy six times during a nine-month period. Unit level training in the preceding months accounts for yet another three to four partial (if not complete) moves involving personnel and equipment.

A few days prior to each detachment, the squadron spaces are disassembled, packed into metal cruise boxes, loaded aboard trucks and shipped (usually across country) to the exercise venue. Included in this awkward procedure are the squadron's inventory of desktop computers – upwards of 30 systems.

As our reliance on computers and their peripherals to conduct our day-to-day business increases, so has our susceptibility to their more than occasional break-downs. Valuable time and money is lost or spent in the repair, assembling, disassembling and shipping of computer systems that were never designed to be moved with such frequency.

The inherent compatibility of laptop computers and sea-going squadrons has been needlessly overlooked. In the rapidly evolving world of computer technology, we struggle in our efforts to procure the latest technology while attempting to maintain a semblance of standardization throughout the Navy. Recognizing the need for a system that would allow rapid dissemination of information between all U.S. forces, the DoD earmarked a PC-based tactical and support warfighting network known as IT-21.

The goal of IT-21 is to link all U.S. forces together in a network that enables voice, video and data transmissions from a single desktop PC. In short, IT-21 sets forth minimum standards for the procurement of computer software. The standards, currently representing front-end market technology, are:

- 200 MHZ Pentium Pro CPU
- 64 MB EDO RAM
- 3.0 GB HD
- 3.5 inch floppy disk drive
- 8X IDE CD-ROM
- Dual PCMCIA/PC Card Reader
- PCI Video with 2MB RAM
- 17-inch monitor (1280-1024)
- Pointing device (trackball or mouse) and keyboard
- Soundblaster (compatible) audio card with speakers
- CPU compatible 100 MBS fast Ethernet NIC

The long-range plan entails outfitting individual squadrons with three such systems serving as shorebased workstations (employing NT server) with the ability to link with compatible systems aboard their respective carrier. In theory, these desk tops would become (post-BRAC) semi-permanent fixtures within their shore-based spaces.

However, IT-21 systems are already being delivered to the fleet. Soon they will be disassembled, wrapped in bubble wrap, locked in metal cruise boxes and transported via truck, hangar deck and up (or down) ladder wells and reassembled in their respective spaces. Some will survive, some will not.

During fiscal year 1997, Strike Fighter Wing Atlantic appropriated $248,000 to outfit the wing and its squadrons with PCs. During the same year, $98,000 was spent repairing these systems. Inevitably, many of these repairs were the result of damage suffered during squadron moves. (The Navy currently doesn't track MIMs (movement induced malfunctions)). Each time a desktop system malfunctions and its repair is beyond the capabilities of squadron or wing ADP personnel, the wing incurs a $200 charge to send the system to FASO, exclusive of any service being performed.

Laptop computers, while both easier to pack and protect, are far less prone to being damaged in a move. Apparently, the people who procure the systems rarely deploy themselves. While 17-inch monitors are nice to look at, they become far less appealing when carried up three ladders.

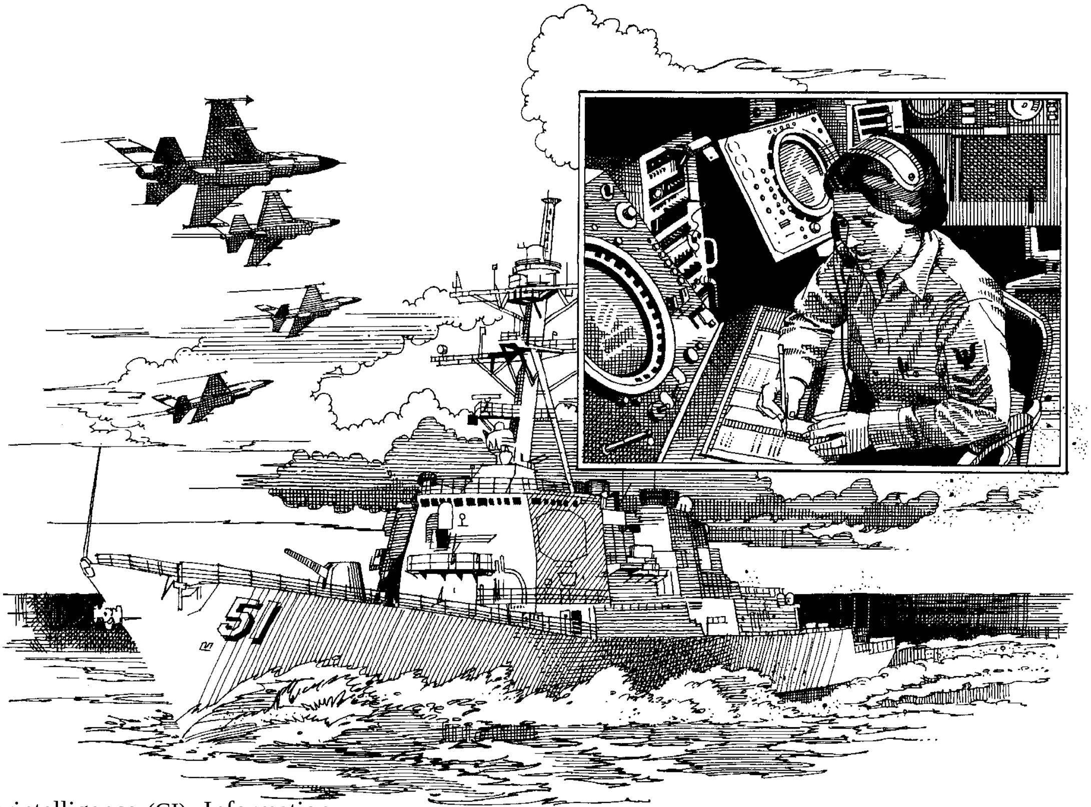
Even after the complete implementation of IT-21, squadrons will still be asked to detach to venues devoid of permanently established IT-21 systems. And while not all squadron desktop systems can be replaced by compatible laptops, the ability to detach with a minimal number of portable systems is far from an unrealistic request.

Currently, there are laptop systems whose design predisposes them to successfully endure a squadron detachment. These ruggedized models are built with a magnesium alloy exterior, are water and vibration/shock resistant and are far less susceptible to dirt and dust. Though slightly more costly than their desktop counter-parts, their ease of movement and enhanced survivability should, over the long term, provide acceptable returns. This technology exists as commercial off-the-shelf (COTS) technology with generous warranty and technological support incentives. If doing it right the first time is a genuine goal, the Navy should analyze the costs and rewards of equipping mobile military units with mobile information systems.

About the Author: LT Brotze is currently assigned to VFA-82 serving as the Air to Air Weapons Training Officer and Operations Department ADP.

Deployable Defensive Information Warfare

By LT Bryan E. Hurd, USN



In a world of diminishing budgets and reduction of bases worldwide, deployment of military units to remote areas has drastically increased. The U.S. European Command faces numerous deployments as part of U.S. Joint Task Forces (JTFs) or Combined Task Forces (CTFs) with international coalition personnel. Unfortunately, the assets and personnel comprising the JTF or CTF are often pulled from the ends of the earth and thrown together in unfriendly environments to accomplish very complex missions.

Personnel in these units are often working together for the first time, with differences in policies, practices, equipment and attitudes on many crucial issues. Defensive Information Warfare (IW-D), Counterintelligence (CI), Information Security (INFOSEC) and Computer Security (COMPUSEC) are no exception.

Additionally, many of the problems cross areas of responsibility by CI support, ADP Security, Intelligence, Operations and Communications offices. Determining interaction and information exchange between these entities prior to deployment ensures effective use of resources in the employment of an overall IW-D program.

Counterintelligence involvement in the planning process and continued support are essential elements of any IW-D program – even more so in a deployed environment. CI provides information on the local intelligence threat and modus operandi of adversaries targeting our information systems and investigates incidents of adversarial intelligence collection, possible loss or compromise of information and security violations. CI input allows security officers to evaluate and improve the INFOSEC and COMPUSEC protective measures and provide mission commanders with on the ground assessments of the effectiveness of the unit's IW-D posture.

It's crucial to evaluate the IW-D posture before the unit deploys. Prior evaluation and decisions regarding the IW-D environment allow security officials to design a protection program appropriate to the mission sensitivity.

In this article, the tenants of INFOSEC and COMPUSEC and their relation to CI will be explored as the foundation to a deployed IW-D program. The issues and examples are a compilation of observations from numerous deployments in the European theater.

PLANNING ISSUES

The planning phase of any operation is the most important time for security and IW-D decisions. Due to the overwhelming nature of primary duties after the start of the operation, most personnel with security as a collateral duty will not have time to plan and consider INFOSEC and COMPUSEC.

The very first question of security should be, "Do I have dedicated INFOSEC, IW-D/COMPUSEC and CI personnel working together on the planning phase of the operation?" If you answered no, it is very likely that your deployment will be plagued with computer viruses, security incidents and violations and will not provide the commanders with an effective evaluation of their IW-D posture.

From an information systems point of view, the planning process should, at a minimum, evaluate the basic areas of communications needs, LAN configuration, information protection, security management, CI and incident reporting and reaction. *The basic questions to ask during the initial planning include:*

▶

Asking the right question is the key

- What type of computer communications and connectivity will the force require?
- Do you require a stand alone LAN, classified connectivity to U.S. or NATO systems or Internet connectivity?
- Do you need to design separate classified and unclassified LANs?
- Who manages the operation and configuration of the system along with its hardware and software?
- What information will be placed on that system?
- Will information be loaded onto the system by diskettes or CD-ROMs?
- Will the system connect to other systems?
- Is the system scanned for viruses?
- Will need-to-know be enforced on the system?

- Who will be given access? (Different nations? Clearance Levels?)
- Who will manage the database of users with access?
- How will clearances be verified?
- Will the requirements for access be enforced PRIOR to giving out logins/passwords?
- Will group accounts be permitted?
- Have users signed a legally binding user agreement?

- Is the person who manages the security of the system in a dedicated position or performing a collateral duty? If your security officer will have numerous other duties, it is likely that the security portions of their duties will be accomplished only after other tasks.
- Is computer security officer assigned as a primary duty?
- Is the person in that job properly trained in computer security, IW-D, CI and related legal issues?
- What policies will this person enforce? How?
- What types of security and monitoring tools will be used?
- Will this person receive threat and intelligence information to support their security program?

- What physical and information security measures will be implemented to protect the system?
- How will diskettes and other computer outputs be labeled and controlled?
- Will users be able to remove, download or upload from the LAN?
- Will this activity be controlled, audited or monitored?
- Are all LAN areas protected from unauthorized access?
- What are the procedures for after hours, cleaning crews, visitors, short term personnel and personnel without proper clearances?

- What is the reporting chain for incidents?
- Who do system operators report intrusions, compromises or violations to? In what format?
- What is the chain of events following a report?
- How is the CI officer involved in incident response?
- How is the commander informed of any ramifications of such incidents on mission safety?

- What entity combines the networks, intelligence, operational, CI and other inputs to give the commander the overall picture of his IW-D posture?
- Do these personnel interact and exchange information on a regular basis?
- Is an operational IW-D working group or cell needed to facilitate communication?
- Who leads this effort?
- What concerns from this entity are brought to the mission commander?
- What is the feedback loop from this entity to the Intel, CI, IW-D and computer network departments?

This list is by no means all inclusive of the COMPUSEC and INFOSEC issues that need to be addressed in a deploying unit, but asking these few questions during the planning stages can save immeasurable amounts of time as the operation progresses.

DEPLOYMENT ISSUES

The deployment of a military force to a remote or hostile location is a very difficult process. The commander must often airlift enough personnel and equipment to effectively accomplish the mission on very short notice. In this process, the commander makes various decisions as to unit size and which essential functions must be operational first. Often, the most important function is communications. Today's communications packages are inseparable from computers. Field units have Local Area Networks (LANs) which allow them to communicate and exchange information with military command units and other organizations.

During deployment, the very first question of security changes to, "Do I have properly trained and dedicated INFOSEC, IW-D/COMPUSEC and CI personnel working together on the protection of my personnel and information in this operation?" If you do not answer *YES*, you have already hindered your ability to implement and manage an effective IW-D program.

Sometimes, in the name of minimizing the footprint of a deploying force, Information and Computer Security personnel are not initially deployed, and their duties are assigned as a collateral duty after the equipment and troops are in the operational location. As a result, the IW-D program will be continually trying to repair previous mistakes or lack of security awareness and activities. No commander would replace highly qualified tank and aircraft maintenance personnel with "a guy who sort of understands mechanical devices." But some commanders appoint "a guy who sort of understands computers" to manage the security of their systems. Each field requires a specialized training curriculum and experience to ensure proper mission accomplishment.

This specialized IW-D officer should work closely with the networks, intelligence, CI and other departments prior to deployment to pull together their expertise and information to give an overall picture of the IW-D posture of the unit and respond effectively to incidents.

Many of the below issues are not specifically the duties of an IW-D or CI officer. However, ensuring the proper implementation of LAN management and media control will avoid countless investigations of suspected loss or compromise from uncontrolled diskettes, virus incidents, uncleared personnel and other issues.

LAN MANAGEMENT

From the above planning decisions on the connectivity needs of the deploying unit, the IW-D officer should ensure that network personnel have a system in place to assist with security procedures and LAN management. Failure to establish the policies and procedures for management and auditing of activities on the LAN from day one of the system's existence, exponentially increases the difficulty of implementing them later.

At a minimum, this management program should include, from DAY ONE:

- A standard hardware and software configuration for all computers PRIOR to connection to the LAN. (Exceptions permitted only with permission of the network manager and COMPUSEC officer.)

- A database of all computer, printer, communications and data storage equipment on the LAN.

- Consideration of whether firewalls, mail guards or other security equipment are needed between portions of the network or on outside network connections.

- A system to track equipment repairs and movements to avoid theft or compromise.

- Consideration of disabling or locking the disk drives on the computers connected to the LAN.

ACCESS MANAGEMENT

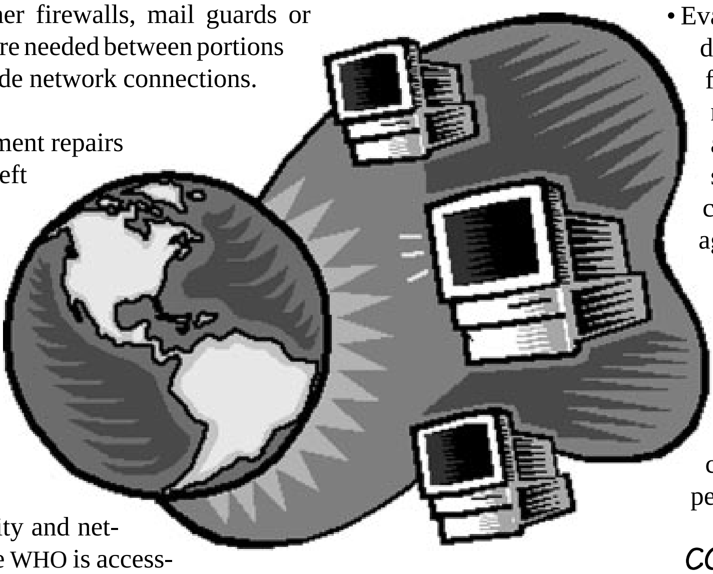
A primary concern to security and network personnel alike should be WHO is accessing the information on my system and any connected systems. *Recommendations for controlling the access to the LAN and its information include:*

- Policies and processes to verify clearances and need-to-know PRIOR to issuing of logins and passwords.

- Software auditing of user activities, including uploading and downloading data or computer programs. (This avoids unauthorized removal of information as well as viruses from unauthorized games or other programs uploaded to the system.)

- A procedure to label and control diskettes and other computer media devices (disk drive locks) or software control of uploads and downloads on each computer on the system to avoid unattended terminals from being used by uncleared personnel.

- Keys for several *access machines*, issued to department security personnel/managers to allow controlled access.



INCIDENT RESPONSE

The lack of a clearly delineated reporting chain for INFOSEC, COMPUSEC or IW-D is aggravated by deploying computer systems and unit personnel. Clearly written and enforced procedures, policy and chain of events MUST exist from the VERY START of the operation to avoid the loss of crucial indications and warning information related to IW-D and CI. *This process should include:*

- Auditing and logging of all user activities and the evaluation for anomalies by network personnel.

- Evaluation of how to proceed in incident reaction that includes input from the intelligence cell personnel, CI officer, Network Manager and IW-D officer. (Evaluation should weigh the concerns of the commander for mission security against the needs of intelligence and CI departments.)

- Maintaining a database of security incidents to allow CI and IW-D personnel to perform indications and warning analysis of incidents and feedback to networks personnel.

CONCLUSION

While these issues may seem basic, in the fast paced world of the deployable JTF and CTF, they are often the first casualties of minimum manning and collateral duties. Issues that frequently eat up time for CI and security departments are often due to lack of a well planned and implemented INFOSEC and COMPUSEC program at the beginning of deployment.

> Addressing the above issues prior to a deployment or crisis action ensures a strong INFOSEC and IW-D Program. Prior evaluation and implementation of the basics will save numerous man-hours for COMPUSEC, network configuration, intelligence and CI while giving the mission commander a better understanding of their actual Defensive Information Warfare posture. A few extra billets at the beginning of the deployment would insure proper use of scarce resources later in the operation.

About the Author: LT Hurd is a member of the 1700 community (Space and Electronic Warfare) and is currently serving as the EUCOM Defensive Information Warfare Operations officer. He has previously served as the NCIS Information Warfare Counterintelligence Threat Program Manager and as a Navy Antiterrorism Alert Center (NAVATAC) Watch Officer. He can be reached at DSN Overseas 430-5018 or commercial 011 49 711 680 5018. His email address is hurd@eucom.mil.

Flexible Local Architecture

By RMCM(SW) Rusty Haynes, USN

Editor's Note: *Instead of spelling out the many acronyms you'll find in this article, we've compiled a list of definitions on page 18.*

DMS is the messaging service of the DII. The DII provides a wide gamut of Information Technology services to meet DoD user requirements. As these user requirements have evolved and matured, the DII has kept pace by continuously evolving. DMS, as an integral part of the DII, must be capable of more than its original functionality of transferring character-based text. It must support a large media menu including imagery, graphics, audio and application specific files. Most importantly, it must be an integral part of DII rather than a stand-alone system. Stovepipe systems are no longer affordable or acceptable!

As initially laid out, the architecture and implementation strategy of DMS limited its flexibility in responding to changes in customer needs and maturing technology. This *Classic Architecture* envisioned for DMS imposed exacting requirements on its user base. Recent trends in COTS development have been away from the X.400 and X.500 ITU recommendations, which were the basis for the classic architecture, and toward the Internet protocols. The philosophy of merging DMS with COTS was suffering as DoD messaging guidelines, in effect at the time, offered little latitude in either design or implementation.

For these and other reasons, the OSD formed an Industry Blue Ribbon Panel to evaluate messaging within DoD.

This panel yielded three findings:

- DoD requirements were moving DMS away from COTS and were instead just building a fancier AUTODIN.

- The explosive growth of the Internet changed the needs of the user base.

- The classic DMS architecture did not allow the use of collaborative computing (GroupWare).

As a result of these findings, DoD issued marching orders to what was called the Flexible Architecture Tiger Team in early 1997. This included finding the means to provide significant acquisition/life cycle cost reductions; defining a more *flexible* framework to support constantly evolving requirements and taking maximum advantage of emergent developments in technology; and improving integration with vendor product plans and leverage off COTS product functionality.

The Tiger Team's solution to these revised criteria for DMS is the GroupWare approach. This is the heart of the new DMS FLA, which has been approved as the current design architecture.

FLA - MORE BANG FOR THE BUCK

The first big change, as you have probably guessed, is GroupWare. Use of a GroupWare product such as Microsoft Exchange or Lotus Notes gives the user significant capabilities and, in some cases, could alleviate or even eliminate the need for a Legacy E-Mail MFI.

Several other new concepts for DMS are incorporated into the FLA. First, the Superserver, a larger capacity server currently being sized at about 2000 users, will be used to host GroupWare Server software. Second, the use of Fortezza with the DMS client will be optional, i.e., the P772 ACP 123 Military Messaging Format may be used without the need for encryption and digital signatures. Fortezza will be an installation configuration option and will still be required for those users requiring the services it provides. Third, the GroupWare packages supporting the commercial version of Legacy E-Mail software, as well as the DMS clients for the same software, may be hosted on the same server. This means when DMS is installed at some commands they can continue to use their Legacy E-Mail as they upgrade to DMS clients over time, and won't be required to add additional hardware (servers) right away.

Figure 1 displays the messaging topology for the new FLA. For those of you familiar with previous versions, two differences are apparent. There is a new name for our old friend, the IMTA. It is now

See the printed copy or web issue for this graphic.

called a LMTA – shown at the left of Figure 1. Next, in the center of the figure there is now a PGWS interfacing directly to a BMTA. In this new topology the IMTA's role has changed. It is no longer the primary interface device between the SMTA and the BMTA. As an LMTA, it serves as an interface device for specialty DMS components such as the MFI, SMS, PUA and MLA. The PGWS now performs the messaging interface to the BMTA. The LMTA is capable of providing alternate BMTA connectivity if desired but will always host UAs for use by the SMS operators. The use of the PGWS, as an interface with other GWSs, allows native formats to be used within the domain serviced by the PGWS and its subsidiary servers providing considerable flexibility for the use of Legacy and DMS User Agents. Interface with other Legacy SMTP users is provided through the inherent SMTP gateway in the server or alternatively through the use of an SMTP MFI for messages that may be Fortezza signed and encrypted.

Under the FLA concept, all users (DMS and Legacy) will have directory information in the DMS directory. As users transition from Legacy E-Mail systems to DMS, their addresses would be updated in the DSA. As shown in Figure 2 below, the LDSA will master local directory information for that location and update other DSTs in the DMS Infrastructure. It also provides directory interface for other DMS specialty products such as the PUA, MFI and MLA through DAP. Finally, it provides directory interface for the PGWS to support directory synchronization for the SAB to the X.500 Directory. Although the server and directory products will be configurable, the user will likely access the SAB for the majority of addressing requests.

The user has three basic options for obtaining Directory information. First, if the addressee has been addressed frequently, their address will likely be resident in the local UAB and will be retrieved from that source. Next, if the addressee is not found in the UAB the UA will search the SAB using native format. Finally, if the addressee is not resident in the SAB, a DAP query will be made by the PGWS to the LDSA and the address retrieved from the DSA infrastructure.

TOPOLOGY SIZING

Depending on the number of users at a site and its geographical location, topologies will range from a single dial-in UA (remote user) to a bank of superservers on a WAN with many specialty components. Under FLA, the very small user would utilize the inherent capabilities in the GroupWare client/server relationship to achieve remote connection via RAS and a modem. Servers for these users would normally be located at a supporting site. If significant internal message traffic was handled at the user site, a GWS could be installed there. The supporting site also houses the DMS components needed by the subscriber for MFI, Directory lookup and MLA services.

The FLA classifies a small site as 51-400 users. In this case, the FLA maximizes the use of native format by the PGWS and other GWSs to handle local message traffic within the GroupWare domain. Messages would only be switched to X.400 when departing the domain for transport over the DMS backbone. The associated specialty components are usually not required at a small site and would normally be provided by a supporting site or LCC.

Under the FLA, 401-3000 users comprise a medium site. Specialty components are justified on-site. The PGWS has two connections to the BMTA: through the LMTA and through the PGWS for redundancy. Behind the PGWS, the messaging infrastructure is exactly the same as for a small site. Only the number of subscribers and servers has changed. This configuration is the nucleus of scalability using DMS GroupWare: adding clients and servers when greater capability is required and leveraging off DMS components in a centrally funded location wherever possible.

The FLA classifies a very large site as greater than 5000 users. PGWS, GWS and DMS components provided in redundancy is the only change from previously described sites. The backup LMTA and LDSA are located at another site to ensure survivability.

WHAT FLA MEANS TO THE USER

The FLA should mean greater flexibility and increased user acceptance. GroupWare functionality when properly applied can significantly improve productivity. Another key advantage is that all command message users will be able to use a common directory. Both DMS and non-DMS users will be listed in the X.500 Directory. DMS users will access certain levels of the Directory using DAP and Fortezza authentication. Future plans call for Directory support of LDAP queries from commercial user agents. Navy projects some two million users will need to be included in its DSA infrastructure.

See the printed copy or web issue for this graphic.

▶

An early lesson learned from the NTDI, our classified DMS pilot in the Pacific, is that DMS system administrators, LAN administrators and Help Desk personnel require a solid working knowledge of the commercial GroupWare of the command's choice (currently only MS Exchange or Lotus Domino) and its associated PC operating systems to fully understand and utilize the associated DMS training that will be provided. Like everything else in the world, acquiring this knowledge base takes both planning and funding. We recommend you consult the web pages for Microsoft (http://www.microsoft.com) or Lotus (http://www.lotus.com) to locate the nearest Exchange or Domino training facility near you, and start sending your key personnel to this valuable training.

This brief overview of FLA shows that DMS is dynamic and evolving. It is considerably more user friendly and *COTS like* than the Classic Architecture. As new capabilities arise in COTS products, such as the move away from UNIX towards Windows NT operating systems and the use of Web technologies and OLE, etc., you can expect to see these capabilities incorporated into future versions of DMS software. One small word of advice: As DMS products undergo rigorous acceptance testing, COTS improvements offered under DMS will likely lag their availability in the commercial sector. DMS will not consciously provide *buggy beta* code to the warfighter for use in combat situations. DMS products incorporating these new COTS improvements will be deployed only after acceptance testing has been satisfactorily completed.

You now have insight into the future of DMS. We hope you're looking forward to these new capabilities as much as we are at the DMS PMO.

Acronym Definitions

BMTA	Backbone Message Transfer Agent
COTS	Commercial-off-the-shelf
DAP	Directory Access Protocol
DII	Defense Information Infrastructure
DMS	Defense Message System
FLA	Flexible Local Architecture
GWS	Groupware Server
IMTA	Intermediate Message Transfer Agent
IT	Information Technology
ITU	International Telecommunications Union
LCC	Local Control Center
LDAP	Light Directory Access Protocol
LDSA	Local Directory System Agent
LMTA	Local Message Transfer Agent
MFI	Multifunction Interpreter
MLA	Mail List Agent
NTDI	Navy Tactical DMS Initiative
OLE	Object Link Embedding
OSD	Office of the Secretary of Defense
PGWS	Primary Groupware Server
PUA	Profiling User Agent
RAS	Remote Access Service
SAB	Server Address Book
SMS	Service Management System
SMTA	Subordinate Message Transfer Agent
UA	User Agent
UAB	User Address Book
WAN	Wide-Area Network

About the Author: RMCM(SW) Haynes is the DON DMS Training Coordinator. He can be reached at (619) 524-7559; DSN 524.

Naval Vessel Register
is Now Online

http://www.nvr.navy.mil

The Naval Vessel Register (NVR) is the official inventory of ships and service craft in the custody of, or titled by, the U.S. Navy. Referred to by Congress in the statutes of the United States Code, Title 10, Sections 7304-7308, the NVR is maintained as directed by U.S. Navy Regulations, Article 0406, of 14 SEP 1990.

Vessels are listed in the NVR when the classification and hull number(s) are assigned to ships and service craft authorized to be built by the President, or when CNO requests instatement or reinstatement of vessels as approved by SECNAV. Once listed, the ship or service craft remains in the NVR throughout its life as a Navy asset, and afterwards its final disposition is recorded.

The NVR has been maintained and published by NAVSHIPSO since 1962. The NVR now exists as an electronic document only. It is maintained and updated weekly. Over 6,500 separate record transactions are processed annually with each being supported by official documentation. The NVR includes a current list of ships and service craft on hand, under construction, converted, loaned/leased and those assigned to the Military Sealift Command.

Other categories include:
- Ship class
- Fleet assignment
- Name
- Age
- Homeport
- Planning yard
- Custodian
- Hull and machinery characteristics
- Builder
- Key construction dates
- Battle forces
- Local defense and miscellaneous support forces
- Status conditions

For more information contact:
NAVSHIPSO
Norfolk Naval Shipyard Det Philadelphia
NAVSEA Shipbuilding Support Office
3751 Island Ave
Philadelphia, PA 19153-3297
(215) 365-5767; DSN 443-1991

How Can I?

The Microcomputer Education Branch of NCTAMS LANT in Norfolk, Virginia provides training and technical support for its customers. Included in this service is answering users' questions. Some of the most recent inquiries are listed below. If you would like further information or have questions you need answered, please call commercial (757) 444-7976; DSN 564. Their e-mail address is training@ccmail.nctamslant.navy.mil. You can look at their current training schedule on the web: http://www.norfolk.navy.mil/training/trainhom.htm.

UNIX

QUESTION: *When UNIX refers to 'rm(1)' or 'ctime(3)', what does the number in parentheses mean? Is it some kind of function call?*

ANSWER: It may look like a function call, but it isn't. These numbers refer to the section of the UNIX manual where the appropriate documentation can be found. You could type *man 3 ctime* to look up the manual page for *ctime* in section 3 of the manual.

The traditional manual sections are:
1) User-level commands
2) System calls
3) Library functions
4) Devices and device drivers
5) File formats
6) Games
7) Special files - macro packages etc.
8) System maintenance and operation commands

Some UNIX versions use non-numeric section names. For instance, XENIX uses *C* for commands and *S* for functions. Some newer versions of UNIX require *man -s# title* instead of *man # title*. Each section has an introduction, which you can read with *man # intro* where # is the section number.

Sometimes the number is necessary to differentiate between a command and a library routine or system call of the same name. For instance, your system may have *time(1)*, a manual page about the 'time' command for timing programs, and also *time(3)*, a manual page about the 'time' subroutine for determining the current time. You can use *man 1 time* or *man 3 time* to specify which *time* man page you're interested in.

You'll often find other sections for local programs or even subsections of the sections above – Ultrix has sections 3m, 3n, 3x and 3yp among others.

QUESTION: *I accidentally created a UNIX filename that begins with a dash "-". How can I delete it?*

ANSWER: UNIX interprets the dash as the precedent to an option/flag. Assuming *-test* is the name of the file

```
rm -test
```

will produce an error message similar to the following, telling you that the flags t e s and t are not legal options for the rm command.

```
rm: illegal option — t
rm: illegal option — e
rm: illegal option — s
rm: illegal option — t
Usage: rm [-Rfir] file ...
```

The simplest answer is to use: rm ./-test

This method of avoiding the interpretation of the "-" works with other commands, too.

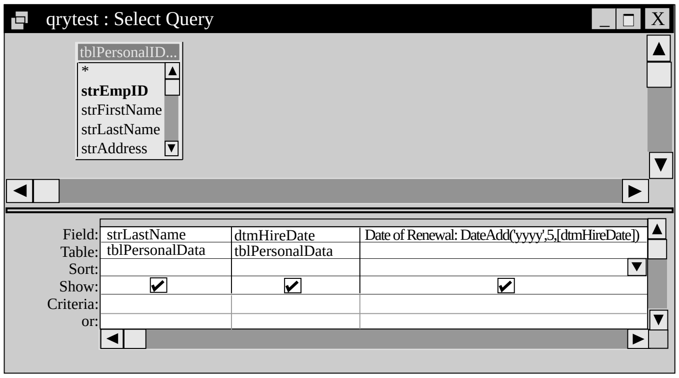
MICROSOFT ACCESS 8.0

QUESTION: *How can I print a report of certification status that will calculate the renewal date five years from the certification date?*

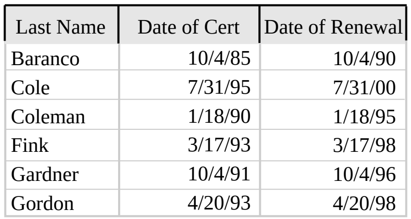
ANSWER: You can do this in either a query or a report. Create a calculated field with the following expression:

```
Renewal Date: DateAdd("yyyy",5,dtmCertDate)
```

This will add five years to the field in each record named dtmCertDate. You can see from the LNC naming convention that this field is of the Date/Time field type.



Field:	strLastName	dtmHireDate	Date of Renewal: DateAdd('yyyy',5,[dtmHireDate])
Table:	tblPersonalData	tblPersonalData	
Sort:			
Show:	☑	☑	☑
Criteria:			
or:			



Last Name	Date of Cert	Date of Renewal
Baranco	10/4/85	10/4/90
Cole	7/31/95	7/31/00
Coleman	1/18/90	1/18/95
Fink	3/17/93	3/17/98
Gardner	10/4/91	10/4/96
Gordon	4/20/93	4/20/98

MICROSOFT WORD

QUESTION: *How can I quickly create a single underline in my form in Word?*

ANSWER: Press the hyphen (-) key three times followed by the Enter key. This will display a thin, single underline across the page width.

Or

Press the underscore (_) key three times followed by the Enter key. This will display a thicker line across the page width.

Or

Press the equal sign (=) three times followed by the Enter key. This will display two thin lines across the page width.

By default, options are set that will allow this feature to function as described. Verify option settings with the following steps:

▶

Make these selections from the menu **Tools/AutoCorrect**...

- Click on the ***AutoFormat As You Type*** tab.
- Verify that the Borders option is activated under the ***Apply As You Type*** option group.

MICROSOFT OUTLOOK

QUESTION: *How can I connect my new Outlook email client so that it will read cc:Mail?*

ANSWER:

1. Obviously, the first step is to install Outlook on the client machine. TO PROCEED YOU MUST CLOSE THE OUTLOOK PROGRAM.

2. *If using WIN95:* Obtain the 16 bit VIM file from http://www.ccmail.com. Unzip the file VIM.ZIP into the WINDOWS/SYSTEM subdirectory.

If using NT4: Obtain the 32 bit VIM file from http://www.ccmail.com. Unzip the file 32VIM.ZIP into the WINNT/SYSTEM32 subdirectory.

3. Run one of two programs on the Office 97 CD under ValuPak/CCMAIL: ccmailnt (for NT 3.51) or ccmailsp (for W95/NT 4). This will install the CC Mail connector.

4. Launch Outlook. Select TOOLS | SERVICES | ADD. Choose MS OUTLOOK SUPPORT FOR CCMAIL.

5. Close and relaunch OUTLOOK at this point.

6. Select TOOLS | SERVICES | MS OUTLOOK SUPPORT FOR CCMAIL | PROPERTIES. *There are three tabs on this window:*

LOGON:	This is where you set the post office path and the user account data.
DELIVERY:	Select appropriate choices.
ADDRESSING:	Select appropriate choices.

7. You are now configured. There is a new option at the bottom of the TOOLS menu bar that gives you additional capabilities to import/update CCMAIL lists.

8. Below are additional add-ins for Outlook that are available from http://www.Microsoft.com/office/freestuff

3 Pane View	Gives a preview of the message
Rules Wizard	For handling incoming messages
Internet Update	Fixes some problems with Internet Mail
Service Release 1	Fixes a whole BUNCH of Office 97 stuff

MICROSOFT EXCEL 8.0

QUESTION: *How do I get formulae to show in cells, instead of the calculated result, when I am using Excel 8.0 (Office 97)? I want to print formulae used so that I can fax them as examples to a colleague.*

ANSWER: Hold down the CTRL key and press the Single Left Quotation Mark (‘) found under the tilde (below the ESC key on most keyboards). This is a toggle. You can also make the following menu selections:

Tools/Options
Click on the ***View*** tab
Activate the ***Formulas*** option under the **Window Options** grouping

Because there are two key combinations that look so much alike, you will want to take note of the additional combination available to speed data entry.

NOTE: If you use the CTRL + (') in a cell, you will get the entry in the cell of the row above repeated. This single quotation mark is located on the same key as the double quotation mark – usually to the left of the ENTER key.

YEAR 2000 ISSUES

QUESTION: *A memo was recently distributed from DON CIO stating orders or acquisition requests for IT shall not be placed against new or existing contracts or other acquisition vehicles unless Y2K compliance is required. The policy applies to orders or acquisitions placed by DON acquiring activities or through other agencies and includes Government IMPAC card purchases. Y2K compliance language in the acquisition vehicle is supposed to hold the supplier responsible for products found to be non-compliant. Where can I get further guidance on Y2K policies, and how do I know which contracts contain the appropriate Y2K compliance language?*

ANSWER: You can locate DON Y2K policy (including the aforementioned memo), procedures, guidance and references on the DON CIO home page at http://www.doncio.navy.mil/ under Y2K Challenge. The DON CIO home page maintains the latest information on Y2K issues and provides links to databases of Y2K compliant products.

The Navy IT Umbrella Program Office is assuring that representative sample testing is being completed by a number of sources to include the OEM and is implementing random testing on actual deliveries. Any non-compliant waivers will be requested through the program office. The following home pages contain information about the programs contracts:

http://www.chips.navy.mil/it/ - Provides information about Navy IT Umbrella Program IDIQ contract/BPAs that are Y2K compliant.

http://itec.part.net/itec.htm - Provides the ability to purchase Information Technology products and services with your Government IMPAC card from Y2K compliant BPAs. Soon this ability will be extended to the IDIQ contracts as well.

The following web sites provide Y2K technical information and lists of IT products that are Y2K compliant. A word of caution when reviewing Y2K compliant databases: An indication of compliance may mean the supplier has stated the IT product is Y2K compliant. Compliance testing may not have actually occurred. To ensure compliance of IT products not previously tested, the prime, supplier, acquisition vehicle management office, or acquiring activity is expected to test a representative sampling of the IT that is delivered and document the results in writing.

http://www.monmouth.army.mil/y2k/comply.htm
Provides information on compliant and non-compliant computers, peripherals, and software.

http://www.mitre.org:80/research/cots/COMPLIST.html
Provides manufacturers Y2K compliance statements.

http://www.mitre.org:80/research/cots/COMPLIANT_BIOS.html
Provides information to determine if a PC's internal clock and BIOS is Y2K compliant.

http://www.mitre.org:80/research/cots/PC_RESOLUTION.html
Provides desktop PC resolution guidance.

Improving the Fleet Sailor's Quality of Life with Library Multimedia Resource Centers

By Karen Stakes

*Several past issues of **Chips** have dealt with the concerns of procurement strategies and vehicles. Each procurement method - BPA, open-market, IDIQ, etc. has its place and function. But, as food for thought, here's what you might call an IDIQ case study.*

Over the past year, I've been involved with a project that at first analysis promised to present more than a slight challenge. As time went on, that initial analysis proved to be correct. We endured many trials and tribulations, but the end result was quite rewarding. Through a partnership effort, it was a win-win situation for all involved.

The project started with a preliminary telephone call from Mr. Berry Patrick, then a program manager at CNET (Chief of Naval Education and Training). Mr. Patrick briefly explained that he was exploring procurement options for the naval general library program. He wanted to provide computer hardware and software for installation aboard Navy ships in support of a CNO initiative to improve the quality of life for fleet sailors. The goal was to establish Library Multimedia Resource Centers (LMRCs) aboard ships. These computer-based centers would be used for the personal growth, professional development, educational support, skill development and recreational enjoyment of the fleet sailors.

The venture would be a joint effort between BUPERS (Bureau of Naval Personnel), CNET and NETPDTC (Naval Education and Training Professional Development and Technology Center). CNET would coordinate the project, NETPDTC would compile requirements based on ships' input and provide implementation assistance, and BUPERS would manage the funding and procurement functions. Mr. Patrick and I discussed NCTAMS LANT PC Store as a procurement option.

Approximately one year later – I thought the project had been back-burnered forever or cancelled all together – Ms. Rebecca Slingerland, Fleet Library Coordinator, NETPDTC, dropped by my office while she was in Norfolk on another project. She said this effort was still planned and that our services would be needed. Finally, in first quarter FY97 a formal meeting between BUPERS, NETPDTC and NCTAMS LANT Norfolk took place. We discussed in detail the services NCTAMS LANT PC Store could provide and the fee associated with those services. At the end of first quarter FY97, we received funding and the go ahead to begin procuring the hardware and software for the LMRC project.

First on the agenda was to clarify the rough hardware and software requirements from NETPDTC. The equipment list included servers, work stations, laptops, CD-ROM towers, laser and deskjet printers, scanners, associated operating system software, an office automation software package and miscellaneous other related hardware. From the rough requirements, we proceeded to the refinement phase – providing expertise on anticipated technology improvements; interface, reliability and durability considerations; and availability of repair and technical support services, etc. Refined configuration specifications were developed and approved by second quarter FY97.

Steve MacMillan,
Fleet Recreation Coordinator Norfolk

"The LMRC program is one of the best initiatives the Navy has developed. The Quality of Life onboard the ship is the most important thing. With this program, it allows families to keep in touch. That's Quality of Life!"

Simultaneously with refining the equipment specifications, we began to develop the overall procurement strategy:

- Should we go open market, BPA, IDIQ contract?
- What manufacturer?
- What vendor?
- What were the lead times?
- Delivery issues?

We needed a contract that offered us quantity availability of reliable, quality hardware and software, delivery to ships anywhere in the world, technical and repair support, integration services, reasonable delivery time frames and competitive prices. We selected the NTOPS and CAD2 IDIQ contracts with Tracor Enterprise Solutions (formerly Cordant).

RP1 Ronald Roberts,
USS FRANK CABLE (AS 40)

"Our LMRC is growing. Due to the demand for the use of this space and the LMRC we should be getting approval soon to expand. This will almost double the size of our present space. This is a great program and the crew stated on a recent survey that this was the best quality of life program!"

▶

From third quarter FY97 through second quarter FY98, we accomplished four separate procurements and deliveries to outfit 292 ships.

SM1 Sid Jones,
USS CORONADO (AGF 11)

"The USS CORONADO LMRC has been up and running since late August '97 and we haven't looked back since. The two month WESTPAC cruise we did in October- November was a great test for us. We were open to the crew 24 hours a day while underway and there were very rare instances when the computers were not being used."

This probably sounds like a typical project, except that the dollar figure might be a little larger than your every day buy. For the most part, that's a true statement. But the biggest challenge came in the delivery phase of the project. It isn't easy to hit a moving target! Folks in the fleet had been hearing about this project for some time and expectation levels were high. Early on, NCTAMS LANT and CNET agreed our delivery goal would be that no ship would deploy without its LMRC hardware. Easier said than done. We started by prioritizing the deliveries based on the ships' scheduled deployment dates. Sounds logical, right? Well, as all those folks associated with the fleet side of the Navy know, deployment schedules can, and do, change at a moment's notice. While this is necessary for the fleet to be responsive to the ever changing world situation, it certainly raises fleet support challenges. We had some close calls and missed initial deliveries to a few ships because of deployment advances. One unforgettable memory was responding to a twenty-four hour notice of a deployment advance. Although the entire team pulled together to make it happen, the delivery missed the ship by a couple of hours.

RP1 Kevin M. VanGorder,
USS WASP (LHD 1)

"Thank everyone involved with the LMRC program. Our crew members spend hours and hours enjoying our computer and video areas."

RPC Gunderson,
USS JOHN F. KENNEDY (CV 67)

"The LMRC computers are a big hit on the ship."

The other real challenge in the delivery phase was to provide ships' tracking information concerning their deliveries and help them trace their equipment en route. We attempted to facilitate this process by sending each ship and receiving activity advance copies of the delivery orders which contained the ships' names, equipment complements, the ship-to addresses along with telephone numbers, and transportation control numbers for the equipment – all the information a ship would need to locate their equipment at the ship-to address. In addition, once alerted by a ship that their equipment delivery was overdue, we would verify that it had left the vendor's warehouse and trace it to the receiving activity, and very often en route to ships deployed overseas. Adding to the frustration level in tracking deliveries was the difficulty in communicating with the ships underway. While electronic mail has helped this situation a lot, very few ships presently have this capability. Needless to say, I have not addressed all the minor glitches we encountered, like the problems that can occur with the mere transposition of a number in a UIC (Unit Identification Code) – a key element in getting supplies and equipment to ships.

Through it all we learned a lot. Some of the *a lot* we learned, I would have given my eye teeth to have known before we started. But, sometimes you don't know what you don't know until you need to know it. So, it's important to be good at recovery. Most of all, I was reminded that more important than a particular procurement method is the importance of a good team in pulling off anything this large and complex. We were truly blessed with a cadre of professionals who handled problems with a *not-a-problem attitude*.

They included:

- The folks at BUPERS who provided not only the funding but guidance on transportation issues.

- NETPDTC who provided the comprehensive project scope and requirements information.

- Tracor who provided the hardware and software, integration services, technical advice and installation assistance to the ships.

- NAVICP Mechanicsburg and the IT Umbrella Contract Managers who facilitated timely equipment substitutions and contract modifications.

- The contract shops and order processing folks who gave our project priority.

- The receiving activities that responded quickly to get the equipment on the last leg of the trip to its final destination.

- And finally, to all those sailors who were patient and supportive as we tried to help them locate their equipment or get technical support.

Speaking for all the members of the LMRC Team, we hope these Library Multimedia Resource Centers make future deployments for fleet sailors a little more bearable and personally and professionally enriching.

About the Author: Stakes is a Computer Specialist working in the PC Store at NCTAMS LANT. She can be reached at (757) 445-4059; DSN 565.

NAVAIR/SPAWAR CAD-2 Contract Overview

Contract Number N66032-94-D-0012

By Kevin Edmonds

The U.S. Navy awarded the Naval Air Systems Command/Space and Naval Warfare Systems Command (NAVAIR/SPAWAR) requirements contract to Intergraph Corporation in 1994. The fixed price IDIQ contract provides an estimated $398,000,000 in computer-aided (CAD/CAM/CAE) products and services to improve engineering design, manufacturing and analysis capabilities for aeronautical, mechanical and electronic design solutions.

This contract is designed to be the Navy's first-stop, total design solutions resource for hardware, software, maintenance, training and technical support services. The hardware and software acquired must support an open systems environment and be Year 2000 compliant. Contract ordering expires in August 2002; maintenance, technical services and training expire in August 2006 at contract expiration. Authorized users of the contract include the Coast Guard and all DoD, federal and civilian agencies.

Initiatives

Intergraph is continually making the NAVAIR/SPAWAR CAD-2 contract easier and more affordable to use. Significant changes have been made to the contract since its inception.

Major changes include:

- Elimination of the once required user funding fees.
- Extending the hardware warranty on Intergraph workstations and NT servers to three years.
- Allowance for all users to make credit card purchases.
- Automatic discount provision for hardware and software purchases that exceed $666,667.

The changes apply to all the NAVAIR/SPAWAR CAD-2 contract offerings by Intergraph.

Products

The NAVAIR/SPAWAR CAD-2 contract has a comprehensive product catalog. *Hardware products include:*

- Engineering workstations such as the powerful state-of-the art TDZ-2000 series 3D graphics workstation for Windows 95 or Windows NT.
- Servers with dual or quad Pentium Pro processors in rack-mountable and non-rack-mountable hardware.
- TD-25 PCs with Pentium II processors.
- Portable MetroBook II and III Notebooks.

Build to order items include:

- Monitors
- Memory modules
- Graphics options
- Processor upgrades
- Disk drives
- CD-ROM drives
- Tape drives
- Printers
- Plotters
- Scanners
- Network and communications options
- Miscellaneous accessories

Software products include:

- Tools for computer-aided design and visualization data management
- Electronics
- Engineering analysis
- Manufacturing
- Mechanical
- Plotting
- System software.

Services provided on contract include:

- Systems integration
- Networking
- Installation
- Warranty programs

Training courses are available to Intergraph product users on-site or at Intergraph. Trained Intergraph consultants are available to provide support services.

Ordering

The NAVAIR/SPAWAR CAD-2 contract procurement process is briefly outlined below:

1. After identifying your site representative, contact Patricia Hail, the NAVAIR/SPAWAR CAD-2 Lead COR.
2. Obtain ADP purchasing approval.
3. Discuss your configuration with Intergraph at 800-747-2232.
4. Prepare your purchase request form. Complete MIPR (Form DD-448), NAVCOMPT Form 2276 or NAVCOMPT Form 2276A.
5. Compile your order package.
6. You will get a faxed copy of your delivery order.

For additional questions please consult Patricia Hail, Lead COR, at 800-305-1662.

Program Contacts

Intergraph
Charlie Brown, Program Manager
Ph: (205) 730-1218
E-mail: slbrown3@ingr.com

Joe Yearta, Technical Manager
Ph: (205) 730-1366
E-mail: jfyearta@ingr.com

Technical/Ordering Questions: 888-671-5339
Fax: (205) 730-6816
URL: www.intergraph.com/federal/

Government
Patricia Hail, Contracting Officer Representative (COR)
Ph: (800) 305-1662 or (760) 939-0615

Madeline Moore, Contracting Officer, Code - 0271.C.3
Ph: (717)790-1701

Robert Donahue, Lead CAD-2 Engineer
Ph: (301) 757-9146

Kevin Edmonds, CAD-2 Engineer
Ph: (301)757-9147

ERM 101: Reengineering Records Management

By Maj Dale Long, USAF

My Command Records Manager (CRM) came to see me this morning. Normally, I wouldn't be worried. He usually drops by to deliver a copy of the Early Bird once he's done reading it.

This time, however, he sat down. That usually means trouble.

Our CRM is a retired Chief Master Sergeant. I learned long ago that having a CMSgt (or a Sergeant Major, or a Master Chief, depending on what service you work in) on your team is a great thing. You simply tell them: "Okay, this is your area. Let me know if something comes up that you can't handle." After that, you basically don't have to worry about them ever handing you a problem.

Unless it's a really big problem. Until this morning, the sum total of the problems that I knew a Chief would bring me was limited to warnings about incoming munitions.

("Sir, get under cover until the shooting stops!")

Since I didn't hear any explosions in the vicinity, I assumed the worst.

He gently placed a copy of the new DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management (ERM) Software Applications, on my desk. But we'd had that for at least a month. This was an issue we'd already been following for several years.

Then I saw the routing slip attached to the top and suffered a brief wrenching feeling in my intestinal tract. Our old buddy Zippy was routing this around for comment.

Now, there are worse things than Zippy being the technical support manager for any project involving computers. But aside from a full-scale thermonuclear exchange or having our sun go nova, I can't think of any others off the top of my head.

After alerting our Computer Emergency Response Team, I walked as casually as I could to Zippy's office. My main hope was that he hadn't had time to acquire any new equipment for *testing*. I've always marveled at Zippy's ability to talk people out of great sums of research and development money on the spur of the moment. I've become convinced that he possesses a highly developed Reality Distortion Field so powerful that it not only clouds how he sees the world, but also projects his warped visions directly into the minds of the hapless people he corners and converts to his causes.

Fortunately, I seem to be immune. Unfortunately, this means I'm sent to deal with him every time he goes on a binge.

There was a small knot of people gathered at the entrance of Zippy's office peeking into the interior, their expressions reflecting various configurations of disbelief and amazement. They scattered like startled deer as I approached, avoiding eye contact. There were some large slabs of flattened cardboard leaning up against the wall.

I had a bad feeling about this.

I held my breath and looked inside the office. Actually, it didn't look too bad. The only new toys I noticed were a large scanner with a sheet feeder, a software box marked *VirtuFile,* and a CD-Recordable drive.

And there was Zippy, busily stuffing stacks of paper into the scanner's feed tray.

He looked up as I entered. "Oh great!" he exclaimed. "I was hoping you'd drop by. Look, isn't this neat?"

He activated the scanner, which started sucking in a page about every 10 seconds.

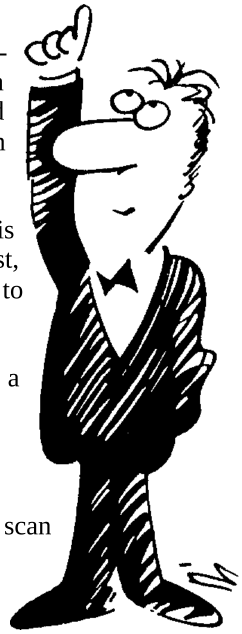
"Yes, Zippy," I replied, "that's very nice. What are you scanning?"

"Why, my e-mail, of course," he said, grinning. "You told me last week that we're going to have to save it all electronically, so it's my first test project."

"Let me get this straight. You printed your e-mail, and now you're scanning it back into the computer?"

"Well, yes. I can add all the information I need about who sent it, who received it, and when, into the records management application database. Look!"

He pecked away at the keyboard for about 15 seconds, entering data in six fields on the input form. The file counter showing the number of records left to annotate dropped down to 34.



"Zippy, everything you're typing is already on the e-mail. Why not just have a program read the *from*, *subject*, *to*, and *date* fields on the e-mail and index them automatically?"

"But this records management software is the only one on the standard products list, and it doesn't do that," he said, pointing to the VirtuFile box.

"Zippy, how many e-mails do you get in a day?"

"Oh, I don't know. Probably 40 or 50."

"And how long does it take you to print, scan and index each e-mail message?"

He counted briefly on his fingers and answered, "About three minutes."

"So you plan on spending two or more hours a day filing your e-mail?"

"I guess so."

He started to frown, which was always a good sign. It meant his RDF was losing strength.

"Okay, let's say we solve the automatic filing problem. Where are you going to store all these e-mail files?"

"Oh, I know there's a lot of e-mail," he replied brightly. "That's why I got this CD recorder. There's lots of room on a CD."

"Zippy, a CD holds about 660 megabytes of data. Do you know how much e-mail traffic we pass over the LAN here every day?"

He shook his head, a pained expression on his face. We'd done this dance enough times before that, a) he knew I already knew the answer to the question, and b) he probably wasn't going to like it.

"There are 2,100 people who work here," I continued. "If we assume that each of them only get half the e-mail you do, about 20 per day, and each e-mail averages 5kb in size, our network deals with 210 megabytes of e-mail every day. And that's not counting attached files. You need to save those, too."

He nodded his head. I could see his distortion field crumbling. The target was locked and I had tone. It was time to finish this.

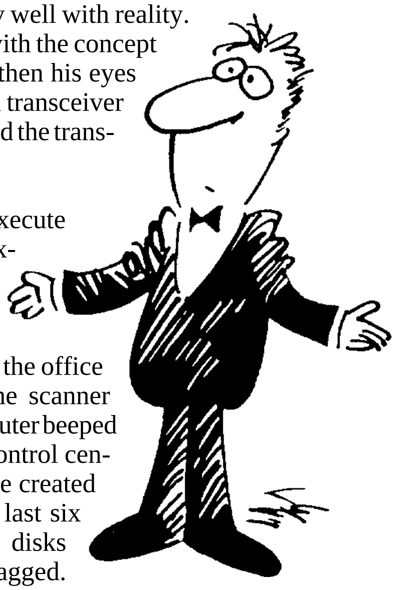
I walked over and placed my hand on the CD-R unit.

"So, you'll have to change the CD every three days to capture all our e-mail. And just saving it isn't enough. You have to be able to retrieve it on demand. Where are you going to store the 200-plus disks the system will produce, and have you got a plan for indexing across the disk volumes?"

Zippy never has dealt very well with reality. His mind struggled briefly with the concept of distributed indexing and then his eyes glazed over. I pulled a small transceiver out of my pocket and thumbed the transmit button.

"Blue Knight to CERT. Execute Plan Scrub Zed. Repeat, execute Plan Scrub Zed."

Three Help Desk techs in beige polo shirts rushed into the office and began disconnecting the scanner and CD-R unit. Zippy's computer beeped plaintively as the network control center remotely wiped every file created on his computer during the last six hours. The VirtuFile box, disks and books were tagged and bagged.



It was all over in less than 15 seconds. The techs evacuated with practiced precision. Zippy's eyes started to focus again about a minute later. He blinked and seemed surprised to see me.

"Oh, hi," he said. "What's up?"

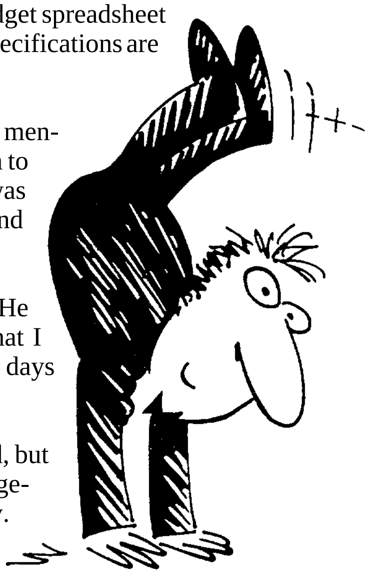
I handed him a floppy disk and a printout. "The boss wants you to rebuild this budget spreadsheet from the ground up. The report specifications are all on this e-mail printout.

Zippy frowned slightly when I mentioned the e-mail, but didn't seem to remember why that reference was significant. He took the disk and read the instructions.

"Wow, this should be fun." He grinned, and settled down to what I hoped would be several harmless days tinkering with the spreadsheet.

Well, that was one problem solved, but only one. Electronic records management is a problem even without Zippy.

So...how the heck are we going to manage 210 megabytes of e-mail records every day?



Records Management: The Basics

Before we tackle any specific electronic records management issues, let's take a brief look at Federal records management in general.

First, what is a record? In the Federal government, records are defined by the Federal Records Act (FRA) of 1950 as:

> "...all books papers, maps, photographs, machine readable materials, or other documentary materials regardless of physical form or characteristics, made or received by an agency of the United States government under Federal Law or in connection with the transaction of public business and preserved or appropriate for preservation by that agency or its legitimate successor as evidence of the organization, functions, policies, decisions, procedures, operations, or other activities of the Government or because of the informational value of data in them."

There are certain characteristics that we assume (hope?) are true for all records:

- That they are authentic, not forgeries.

- Once entered into a system of records, they may not be altered.

- That the information in a record is of some value to the organization.

Records management has been part of the fabric of government for decades. It has survived relatively unscathed despite the advent of photocopiers, microfilm, microfiche and various other new information technologies. Now, however, networks and personal ▶

computers may shake records management to its foundations. What makes this technological assault different?

Paradigm Shifts

The greatest constraint to managing information this century has been the file folder. It has dominated all our thinking about how to organize and retrieve information, even to the point that we store digital files in *folders* on our computers.

The basic premise of a folder is that a file will always exist as a discrete object at one physical location. It may be copied and distributed many times, but work involving paper files is more often performed sequentially, with one person using the information and then passing it on to the next person in the chain.

The introduction of networks and shared files are starting to disrupt the old *information can only be one place at a time* paradigm. A file on the World Wide Web, for example, is available simultaneously to millions of people who do not disturb or remove the original document when they view it. Many of our current records management mechanisms are designed to preserve the integrity of the original copy of a record. If we can make electronic records freely available without risk to our archives, we may be able to eliminate a significant portion of our old process cost.

Even more radical, though, is the idea that some electronic record material may only exist in a set form at the time it's viewed, and not continuously. Tables containing personnel, financial and equipment information, for example, may all be maintained separately as independent records. However, information from these tables may also be joined to form lists of who maintained or purchased particular pieces of equipment.

Need a current list of all the equipment signed out to a particular person? In a paper world, we might go to a filing cabinet and pull out one or more hand receipts that show the information.

In a digital archive, however, we could query the database and have it assemble a list of his inventory for you on your monitor. However, when you close that report it no longer exists as a discrete entity, unlike those paper hand-receipts. The query that retrieved it may not even be stored anywhere if the requester doesn't specifically save it.

I would submit, though, that preserving access to the inventory information in our example without having to keep permanent physical or virtual files with that specific information meets the objectives of the FRA. Yes, it will take a more sophisticated audit system than we have at present to manage all those tables and relations, but what would be a virtually impossible task in the paper world can be handled in the background by a computerized records management application (RMA).

Providing, of course, we understand records management requirements well enough to tell the RMA what it needs to do.

Hide and Seek

In addition to changing the rules of access to records, networks and databases introduce a second major disruption to the status quo.

How do we find records? Under our traditional system, you have to know where to look to find what you need. Do you have trouble finding a particular record series when navigating that file plan your clerk set up? And, having found it, do you groan in pain when you discover the material in the cabinet fills two linear feet and is indexed chronologically when you're looking for information by subject?

In an electronic record set, documents can tell you where they are through information brokers like structured queries and computerized indexes. A simple, properly-structured query or index search should have record filenames politely lining themselves up on screen for your review without a single paper cut on your finger.

We can only index a paper record set on one aspect of content, usually alphabetically, chronologically, by subject, or some similar identifier. However, we can index or search for electronic records based on virtually any aspect of their content. This is a tremendous mechanical advantage.

Practical Applications

Now, back to my earlier question: What are we going to do with all of our electronic mail? We probably generate a terabyte or two of e-mail every day throughout DoD.

First and foremost, the courts have decided that if the content of an e-mail meets the definition of a record, we must manage it as record material. This has been unanimously upheld from Federal district court through the U.S. Court of Appeals.

Second, the courts have also ruled that printing e-mail and trying to use the paper copy as the official record does not meet the requirements and objectives of the FRA, as the paper copy does not contain all the characteristics of the original electronic version.

As e-mail becomes more acceptable as a means of official communication, particularly as part of the Defense Messaging System, it will assume a larger share of our total communications over time. The time to figure out how to manage e-mail records is now, while we still have time to design the capability into the initial DMS implementation.

Managing the Flood

I have two proposed rules of engagement for e-mail records:

- We must archive e-mail electronically.

- We must find a low-maintenance way to manage both the archival and retrieval processes.

First, we have to decide what e-mail we're going to save. After some consideration (about three years worth), I've come to the conclusion that it will be better to just automatically save all our e-mail instead of asking users to decide what to save or not to save. Now, before all the network administrators in the audience start reaching for their heart medication or weapons, let me explain exactly what I'm proposing.

DoD records management policy makes the originator of a document responsible for managing the record copy. Therefore, my first premise is that we primarily need to save what people send, not every e-mail they receive. This cuts our inventory down a bit, as it should eliminate storage of duplicate copies sent locally.

We may want to save some of what we receive from outside sources, so the system should also capture and archive incoming e-mail. A mechanism to identify and eliminate duplicate copies is essential, but we already have automated ways to do this with incoming AUTODIN message traffic, which should be transportable to our e-mail archiving system.

The combination of the two should result in an archive of 100 percent of our e-mail traffic without saving duplicates.

We will need a tremendous amount of storage space. I'd suggest either extremely large hard disk arrays or CD-R jukeboxes. Storage media costs have been decreasing by over 25 percent per year for the last four years, and commercial deployment of CDs that will hold 4GB of data per disk isn't that far away. Both solutions include the technology to index the entire archive, and CD-R *write once, read many* technology may give an added measure of data security.

Save Everything?

Why save it all automatically instead of letting all the users decide what to do with it?

First, any e-mail that is a *transaction of public business* is record material. We work on government equipment, most of which should have warning notices that include the phrase, "use implies consent to monitoring." Our policies for e-mail use should include guidelines for *acceptable personal use* of these systems, usually based on some perceived benefit to the government, so even personal e-mail sent from work may be considered *official business*.

Second, doing anything manually that a computer system can perform automatically is, to me, a gross waste of time. Asking someone to make a records management decision every time they send an e-mail would be both annoying and inefficient. If our electronic records management systems are not largely ubiquitous, they will not be effective.

In saving everything, I include all those word processing, spreadsheet and presentation slide files people keep attaching to e-mail in an attempt (at least according to our LAN administrator) to overload our mail server. However, as those documents are part of the total transmission, they need to be saved as part of the package.

Tweak the e-mail server and the firewall to ship copies of the e-mail we want to save to a dummy account configured to dump the e-mail and attachments to a storage device. Run an indexing engine on the storage area periodically to help people find the e-mail records they want to review.

If you're concerned about 2,000 people having access to the entire e-mail repository, then limit access to the organizational e-mail archive to your appointed records managers. Most people will save e-mail they consider important to them on their own computers. While that's handy for them, it doesn't help us meet our organizational responsibility to preserve and manage the sum total of our e-mail.

Finally, set a final application to watch for e-mails to queue them for disposition review. This could be as simple as a file manager window that sorts by date or as complex as a fully indexed relational database.

DoD Requirements

Complicating my plans, however, is the new DoD 5015.2-STD, Design Criteria Standard for Electronic Records Management Software Applications. A text version of the standard is located on the web at: http://web7.whs.osd.mil/text/p50152s.txt.

(There are also PDF, SGML and MS Word versions, but the text one loads a lot faster and reads the same.)

DoD electronic records management systems must be tested and certified by the Joint Interoperability Test Command (JTIC), which is part of DISA. Commercial-off-the-shelf (COTS) records management products that pass the certification test will be placed on a formal Records Management Software Applications Product Register. All software products for records management purchased by DoD are supposed to be certified and listed in this register.

The standards themselves are fairly easy to follow. It's the systems approval process that concerns me. As it stands now, software vendors can pay to have their records management software tested and added to the register if it passes. However, this could restrict our choice of applications to only those provided by whatever vendors choose to participate. While I'm a fan of the concept of using COTS whenever feasible, I'm not sure I want my systems choices driven solely by what vendors are willing or able to provide.

I would hope that JTIC will extend testing and certification services to DoD organizations that come up with good ideas for RMAs. If we can meet a portion of our requirements with tools that we already have on hand, I see no reason to spend millions of dollars on duplicate mechanisms because only vendors were willing to test their ideas.

The Key Piece

As the document is the foundation of current records management practice, digital signatures will be the foundation of any electronic RMA. Lack of a widely-implemented digital signature standard is currently our biggest barrier to electronic record-keeping.

From a legal standpoint, a signature serves as proof that someone deliberately signed a document and convinces the reader that the document is authentic. It is part of the document and cannot be transferred to another document. Once signed, a document is supposedly unalterable. Finally, authentic documents and signatures are physical objects and cannot be repudiated by the signer.

We accept those statements as true for signatures on paper documents, though signatures can be forged, physically transferred ▶

from one piece of paper to another, and don't really protect someone from editing a document after it's been signed. Thus the need for witnesses or Notary Publics for really important documents.

Digital signatures, on the other hand, can reliably do all these things on their own. A digital signature is a string of bits generated by the signer attached to an electronic document. The bit string is based on the signer's personal keys (public and private) and the document's data. Authenticity can be proved by validating the document with the signer's public key. Any changes to the document will invalidate the signature and allow the signer to prove that he did not sign the altered version.

DMS will have this type of signature capability, but it isn't the only system that will generate electronic records. Coordination, correspondence, electronic commerce and any other process we may want to conduct electronically that needs digital signatures should incorporate the same digital signature system that we use for DMS.

Or DMS should incorporate theirs. As long as the signature system works, I really don't care whose standard we use. A standard digital signature solution should be part of all our operating systems and applications, not developed piecemeal for each new system we bring on-line.

Other Issues

E-mail, I'm afraid, is only the tip of the electronic records iceberg. As we use more electronic forms, there should be some movement towards capturing all the data entered on them in databases. Computer applications routinely produce internal files that may meet the definition of a record without ever intending to.

World Wide Web browser history files, proxy server logs and firewall logs document our organizational Internet transactions, and may meet the definition of Federal records, as they are very similar in nature to telephone logs that record when and where we make long-distance calls from government phones. There is currently a court case in Tennessee addressing this very question, and government organizations in Arizona, California and Florida have already provided access to browser history file information due to requests from the public.

There are probably quite a few applications currently in use that produce some type of digital information product or by-product that would qualify as Federal records material. Hopefully, the discovery process won't be too painful.

In closing, I foresee two phases in electronic records management over the coming years:

Phase 1: Automation

In this initial phase we will, for the most part, automate our current records management procedures. Electronic files will still be treated as discrete objects in our archives and filed in electronic folders, just like virtual filing cabinets. There will be few changes of any note to records management policy. Some security and authentication systems will probably be unique to various applications and not compatible with each other, creating new stovepipes to consolidate later on.

Functional managers will try to maintain separate RMAs for what they consider proprietary records, such as personnel and financial data. This will be a crucial test of our resolve to build a true organizational repository. Everyone has to play by the same records management rules, and the advent of mass storage and virtual access allow consolidation of our archives. Instead of having everyone manage duplicate RMAs, there should only be one for any given organization or location with all the rules programmed in one place. Satisfy the functionals' need for control and security of their operational data at the system level, but maintain the RMA centrally.

There will be good things happening in this phase. Anything that can be automatically assigned to a record based on existing procedure should be. Any task that can be automated should be. An example of this will be the use of *smart folders*. You should be able to drop a new record in a virtual folder and have the RMA automatically assign all the record information (file codes, disposition instructions, etc.) that we now have to do manually. Electronic indexing will make finding records much easier. The RMA will handle all the auditing and disposition automatically.

This will seem like the end to some people, but it will really just set us up for:

Phase 2: Relation

The principal characteristic of this phase will be the ability to merge information from previously discrete sets of information into relational entities. The enabler at this point will not be hardware or software, but an enterprise data dictionary and use of standard data elements in all systems that produce electronic records.

There will be significant shifts in policy to take greater advantage of relational and object-oriented technology. We will have one digital signature standard implemented across all our applications, and system security will know the type, status, and condition of every user, component, and piece of information in the system. Organizational archives will be centrally located, but individual files and data will be managed from wherever appropriate. There will be no redundant data; changes made to any piece of information will be instantly available to everyone else sharing the data store.

This is not metaphysics; all the technology for Phase 2 is available today. Our main handicap is that we have a lot of inanimate inertial mass (dead weight) from decades of *managing by file folder* and built into proprietary information systems. It's going to take a lot of pushing and shoving to get this moving.

Leveraging Technology

The Greek mathematician Archimedes once said, "Give me a lever long enough, and I will move the world."

In this case, technology is our lever, and understanding the legal requirements of records management our fulcrum. If we can keep the two in balance and use that leverage, Phase 2 shouldn't be that far away.

About the Author: Maj Long is the Chief, Command Information Management, United States Strategic Command. He holds a Master of Science degree in Information Resource Management from the Air Force Institute of Technology.

Chips Choice Web Site Review

By Elizabeth Dickason

Introducing the Chips Choice Web Site Review - spotlighting a .mil web site that provides well-presented, useful information with the right amount of style.

I thought it would be a good idea to start highlighting some of the well-done .mil web sites in ***Chips***, since a large majority of the free world, including the military, is jumping on this 21st century bandwagon. Being a Navy-sponsored magazine, I decided to start with a .navy.mil web site.

I have a few Navy sites bookmarked, but to get a better feel for what's out there I started browsing the web. I went to Navy Online (http://www.ncts.navy.mil/nol/) since they have an extensive listing of Navy web sites. From there, I found several sites that caught my eye. As we've all been told, first impression is very important. Conclusions are drawn from that first meeting. This held true in my search for a web site I'd like to review. Those with eye pleasing qualities made the keeper list. After reviewing about fifty plus sites, I narrowed it down to my top three choices. From there I considered content, layout, organization, loading/viewing speed and overall quality.

I've kept you waiting long enough. The Chips Choice Web Site for this issue is Military Sealift Command (MSC). Their web address is http://www.msc.navy.mil. I liked the color scheme, slide show and layout. From there I found the site easy to maneuver through – with a built-in site search engine as an added bonus.

They've cleverly taken the acronym for Military Sealift Command and made a slogan: **M**ission: **S**ervice to **C**ustomers. The main screen has a black background with rainbow lettering in what looks like the Mistral font. The main menu choices are shown on the left hand side of the screen, with a slide show highlighting various command functions running on the right. The slide show, which includes seven pictures that change approximately every ten seconds, is shown in a cloud-like frame instead of the standard rectangle or square. This adds a nice touch. A caption runs with each slide. A grey ship silhouette is embedded in the background and appears on all the other layer pages as well. This adds continuity to the style of the site.

Let's look at the criteria I chose and the importance of each:

Content

The saying, beauty is only skin deep, fits this category well. Just because a web site is nicely designed, doesn't mean it has anything to say. Was the information easy to understand? Did you find what you were looking for or learn anything new? Was the information useful enough that you will return to the site again? If you answered no, then the site has failed the content test. Since the web's main objective is dissemination of information, if you fail this category your web site is in big trouble.

The MSC web site is filled with good information. Working for the Navy, I've heard of MSC but never really knew what they did. I now know that they are a world-wide organization headquartered in Washington, D.C. employing more than 8,000 people, both military and civilian. The command is responsible for ocean transportation of military supplies and equipment; providing seagoing platforms to support special at-sea missions; and logistics support to U.S. Navy ships at sea.

The site includes an MSC world-wide phone directory and ►

information on employment opportunities, as well as a clickable organization chart and available procurement opportunities.

Layout

Layout is especially important for first-time visitors who are unfamiliar with what a web site has to offer and where to find it. The MSC web site has eight main topics that breakdown into several other layers.

Their eight main topics are:

- Mission
- Commander
- Organization
- Requirements
- Contracts
- Employment
- Personnel
- What's New

If you're a regular visitor to this site, you'll probably want to check out the What's New section first and go from there.

While a rectangular header runs at the top of each sub page, the shaded image changes to reflect the theme of that page. For example, the rectangular header at the top of the personnel section shows some of the many faces of the command; The requirements section header relates to cargo.

My least favorite screen on this site is the Organization page that shows a flow chart of their organization. There are two color schemes on the chart. The blue boxes with yellow type signify that they're clickable. The grey boxes with yellow type are not. Showing the two variations in color is a nice idea, but I suggest changing the yellow text on the grey boxes to another color, or using a skinnier font. That text is very hard to read.

Organization

MSC's web site is very user friendly. A search engine is available at the bottom of every page – so if you know what you're looking for but aren't sure where to find it, just search and ye shall find. I typed in the word *employment* and got 230 matches. If I was really serious about searching, I'd need to search for a more specific topic. In addition to the search engine, the main menu choices appear at the bottom of every page.

I never felt *lost* while I was on this site. The sub layers aren't so deep that I couldn't find my way back to the surface. The mission section, which seems to have the most subsections, has a navigational set of up and down arrows, showing you where you are in comparison to the other sublevels in the mission category. That's nice – I always travel better with a map.

Loading/Viewing Speed

Not everyone in the military is viewing the web from a Pentium. It's important to remember that when designing a web site. Those less fortunate souls are the ones who suffer when a website is loaded too heavily with graphics. The frustration associated with the slow load time is enough to turn alot of otherwise good customers off. I've been to many web sites where I've hit the Stop button because the wait for loading is just too long.

Some advice: if your web site requires a lot of graphics to get its point across, make some of them clickable choices instead of embedding them. Let the viewer choose when to view the graphics.

The MSC web site loads quickly and is not overburdened with graphics. They keep a common design theme throughout the site. The header bar, which is nicely designed, allowing for subtle changes for each category title, adds a nice touch without being too overbearing. The standard white background with black text for most of the pages is easy to read.

Some supporting pages do have graphics, but the quality of the photos and load times were good.

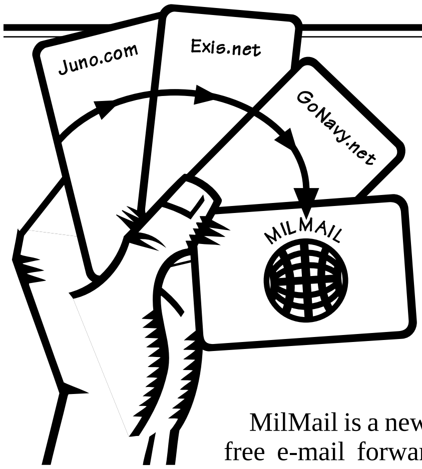
Overall Quality

This category ties it all together. If the overall quality of the site is good, chances are people will bookmark the site and visit again – and isn't that what you're hoping for? As long as the information is updated regularly, the links stay current and the site is technologically competitive, visitors should be pleased.

The MSC website meets all the above criteria. I liked the look and feel of what was there and the way it was presented – straightforward with a consistent but classy design. I definitely learned something from the information they presented.

If you've seen a .mil site that stands out as a winner, email us at chips@email.chips.navy.mil. Others may think it's a winner, too.

About the Author: Dickason is the Assistant Editor of Chips. □



Moving Forward with MILMAIL

By Peggy A. Neil

MilMail is a new, commercially sponsored, free e-mail forwarding service intended for active-duty, retired and reserve military personnel. If you register with MilMail, you can change your e-mail provider yet keep the same MilMail e-mail address. MilMail will forward your mail, excluding attachments over 500kb, to your current email address. This maximum attachment size won't interfere with most users' needs, but will exclude sending large files, such as certain executable programs (i.e., netscape.exe).

E-mail forwarding services will benefit you if you change your e-mail provider-of-choice/ISP (Internet Service Provider). For example, if your current ISP is Juno.com, and you're registered with the MilMail forwarding service using one of its domains – we'll use GoNavy.net – your friends can send your mail to GoNavy.net and it will still reach you. MilMail will forward it to you so when you log into Juno.com, your mail will be there. If you decide to switch your mail account to Exis.net and notify MilMail of your new Exis.net address, your GoNavy.net mail will now be picked up from Exis.net.

Essentially, if your friends use your MilMail address to send you e-mail, you can switch e-mail providers, register your new e-mail address with MilMail and your e-mail will automatically be forwarded to your new e-mail address. Some e-mail providers allow you to specify your return mail address. If your e-mail provider permits this, then you can indicate your MilMail address as your return address. Certain other providers, including AOL, Compuserve, and Prodigy, have no such provision so that anyone who saves your address or sends you return mail will bypass MilMail forwarding. Your mail will go directly to whatever account your original message came from unless your friends manually enter your MilMail return address into their messages or address books.

MilMail's press release claims to have more than 4,000 military-oriented domains to chose from. I'll take their word on the number of domain choices they offer, but there does seem to be plenty of military oriented options including ranks, ship names and submarine names.

A domain name is a location on the Internet, similar to the *state* part of your mailing address, that is written on the right of the @ sign such as mymail@GoNavy.net. Top level domains are given certain set extensions: *.net* for Internet Service Providers and *.mil* for military organizations. Most of MilMail's domains end in .net because MilMail is an Internet Service Provider – a commercial business that isn't affiliated with the military.

Table 1:
Some of the Military Oriented Domain Names Available Through MilMail:

United States Navy / United States Naval Academy
Navy.org
GoNavy.net
USNA.net
Midshipman.net

United States Army /United States Military Academy
Army.net
GoArmy.net
Infantry.com
Soldier.net
USMA.net

United States Air Force/ United States Air Force Academy
USAF.org
AirForce.net
USAFA.com
Cadet.net

United States Marine Corps / United States Naval Academy
USMC.net
Midshipman.net

Table 2:

What's a domain name?

A domain name is a friendly interface to the numerically-based IP addressing system. The top level domain describes the type of activity used by the name holder, e.g. **.com** for a commercial activity or **.net** for Internet Service Providers. The specific internet site is then identified to the left of the top level domain e.g. **GoNavy**.net. The period that separates the two levels is pronounced *dot*.

The primary top level domains are:

.com - Companies
.net - Internet Service Providers
.edu - Educational Institutions
.mil - Military
.org - Non-profit organizations
.gov - Government

▶

While MilMail doesn't require web access to use its services, the only way to sign up for the service or update your ISP is via their web site (http://www.milmail.com). If you don't have web access on your PC, you'll have to find a friend who does or visit your local cyber-cafe to complete their registration process. The application for MilMail currently includes an extensive questionnaire with a number of required elements such as marital status, education, number of children, employment status, job function, household income, date of birth and a list of *general interests* (such as sports, technology and gardening). MilMail's founder and president, Colby D. Fisher, explained that all this information is strictly reserved for internal use and isn't available even to the MilMail sponsors. In addition, the registration questionnaire is currently being rewritten with more open-ended questions.

When I registered my dad for the service – he's retired military – I found that *company size* and *job function* are required responses even if you show your current job status as *retired*. Too bad taking care of the grandchildren wasn't a possible choice under job function. I ended up registering him as Executive/Senior Management for a company of less than 10 employees. I guess that description will fit for him or Mom!

One option in MilMail's sign-up process is to block incoming mail from what MilMail refers to as *many of the notorious spammers*. Spammers are people who blanket thousands of e-mail accounts/newsgroups on the Internet with unsolicited messages having nothing to do with the recipients. These messages are generally of the *MAKE MONEY FAST* variety. Their actual purpose is *denial of service* – which results when these annoying and illegal messages flood the Internet. Most Internet e-mail users will relish the opportunity to decrease spam mail.

An additional MilMail feature offers those with homepages the use of a permanent homepage address. This feature provides forwarding to your actual address, much like the e-mail feature forwards your mail to your actual e-mail account. MilMail also offers free space for homepages for qualified military units and organizations. You can see an application for an organizational homepage at http://www.navy.org/homepage.htm.

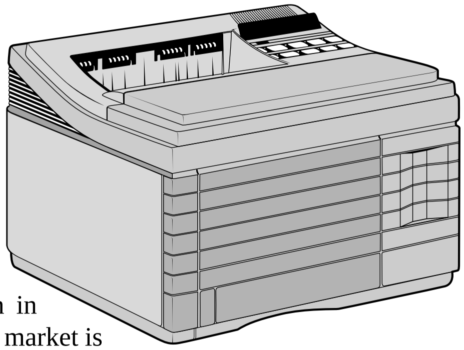
How can MilMail afford to provide these services free of charge? It is supported by various advertisers. When you sign up to use MilMail, your name is added to an internal mailing list. When MilMail receives information about specials from its sponsors, it forwards this information to everyone on its internal mailing list.

To see if MilMail meets your needs, access their web site at http://www.milmail.com.

About the Author: Neil is a Computer Specialist at NCTAMS LANT. She can be reached at (757) 445-0072; DSN 565.

Color Printing: To Print or Not To Print?

By Patrick Koehler



In the spirit of Patrick Henry, who said *yes* to the fight for independence, I would have to answer the title question, *Color Printing: To Print or Not to Print,* with the same brave *yes*.

Color printers are coming down in price – the average range in today's market is under $200 for a 600 dpi color inkjet to $8K for a high quality dye sublimation printer. Even popular color laser printers such as the HP Color LaserJet, Tektronix Phaser 560 or Xerox 4915 Plus can be purchased for under $4K.

The questions really boil down to what type of technology do you want? What quality do you need? How fast must you have your output? Let's take a look at some of the questions before you say yes to a particular color printer.

What printing technology should be used?

Inkjet printers are the least expensive color printers. There are two basic types: thermal and bubble jet.

The thermal printer uses a heating element in the print heads which displaces volume and pushes ink out the opening. The bubble jet uses a piezo crystal, which vibrates when an electrical signal is applied forcing the ink out.

Output can be great with a dpi (dots per inch – explained later in this article) of 1200 x 1200 on a Lexmark 7000 or 1440 x 720 with an Epson Stylus Color 800. The output quality of ink jets can be *enhanced* by using coated papers. Standard paper can be used, but bleeding may occur when printing solid colors at the highest available resolution. By using a heavier weight, glossy paper, bleeding may be non-existent.

The ink for these printers is water soluble, so care must be taken not to get prints wet or they'll smear. Typically, inkjet printers perform quietly, but are slow compared to standard laser printers. Some inkjet printers such as the Tektronix Phaser 140 offer a network connection via a LAN card or can be shared using Windows v3.11, Windows 95 or Windows NT.

Inkjet printers, such as Cannon, use four separate color cartridges (black, cyan, magenta, yellow) while Hewlett Packard uses two cartridges (black and a combination cartridge of the four colors). The Epson Stylus Photo uses six colors: the four basics plus light cyan and light magenta. Inkjet technology is low cost with professional output.

Laser printers use a toner-based product similar to standard black and white laser printers. Typically, a color laser printer uses black, cyan, magenta and yellow toner cartridges. Each type of laser uses slightly different printing mechanisms. However, the *typical* color laser applies a static charge to a photo

continued on page 38

Purely Polymorphic

By LT Rick Miller, USN

In the January 98 issue of ***Chips***, I presented some of the basics of object-oriented analysis, design and programming and showed how this design methodology is used to tame the complexity associated with modeling real-world problem domains. But to gain the full expressive power of C++ and object-oriented programming in general, you'll need to understand the concept of polymorphism. (That is pure polymorphism as opposed to ad hoc polymorphism which is operator overloading.) In this article I'll show you how to write polymorphic C++ code. But first, what is polymorphism?

> A good definition of polymorphism is "The ability to operate on and manipulate different derived objects in a uniform way...." (Sadar) Add to this the following amplification: "Without polymorphism, the developer ends up writing code consisting of large case or switch statements."..."This is in fact the litmus test for polymorphism. The existence of a switch statement that selects an action based upon the type of an object is often a warning sign that the developer has failed to apply polymorphic behavior effectively." (Booch)

Polymorphism in C++ is achieved through the use of virtual functions (pure or nonpure), base classes, inheritance and pointers. A base class is declared with an interface consisting of pure or nonpure virtual functions. If one or more of the interface methods in a base class are declared as pure virtual functions, then the base class is referred to as an abstract base class and no objects of that class can be instantiated. However, where a reference to an abstract base class appears in the source code as a return type or parameter type, etc., a derived class object can be used in its place. Although an abstract base class object cannot be instantiated, a base class pointer can be declared and initialized to point to a derived class object.

To illustrate, I'll design a fleet of computer-controlled vessels. Each vessel will utilize a power plant and an array of weapons. An Admiral in command of such a fleet will obviously need to send orders to the vessels like "Fire Weapon!", but shouldn't be bothered with the details of how each different type of weapon works. Just like the Automobile example I presented in my last article, the interface to vessels will be the same regardless of whether the vessel is actually a surface ship, submarine or orbiting space weapons platform.

Figure 1 is a static diagram in Booch notation for the classes

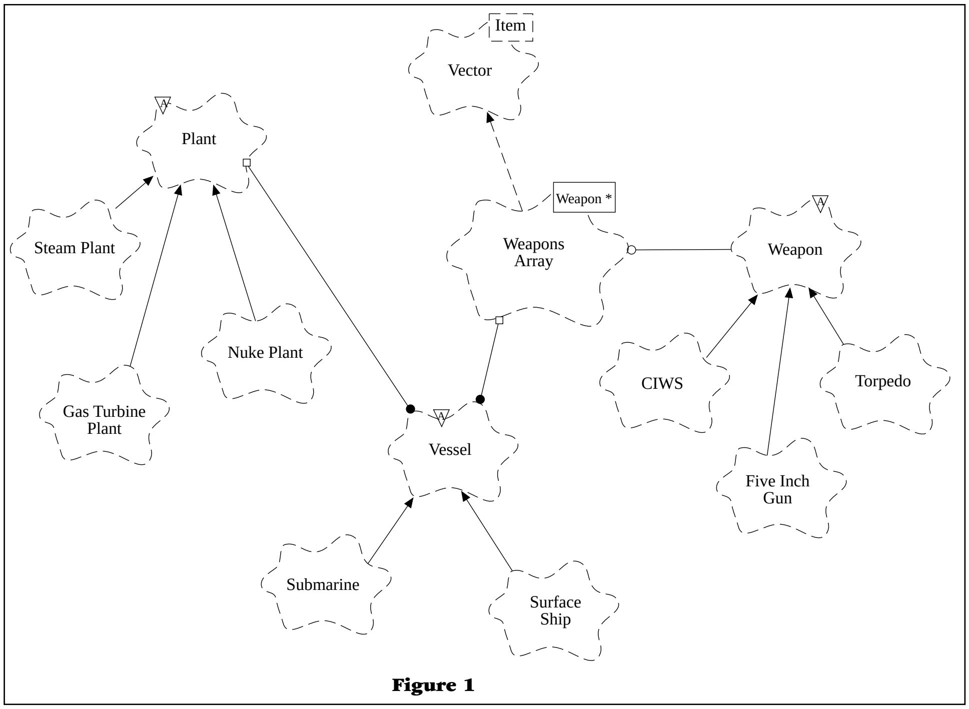


Figure 1

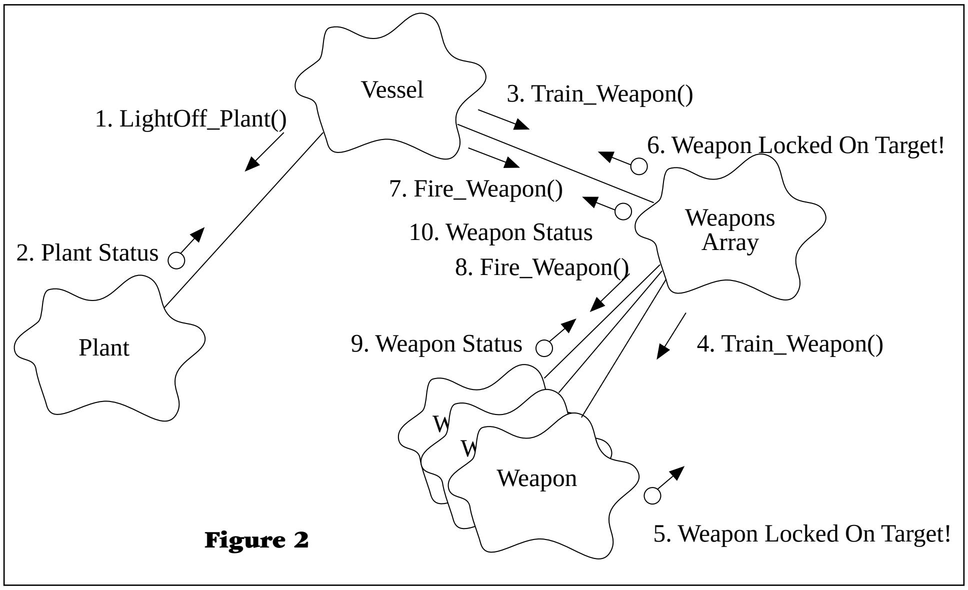


Figure 2

►

comprising the computer-controlled fleet. The three primary classes include: Vessel, Plant and Weapon. The "A" in the triangle that appears on each of these classes is an adornment indicating these classes have one or more interface methods declared as pure virtual functions. Again, what this means is these classes exist simply to provide a common interface to any class that derives their interface.

The Weapons Array is a special case. The C++ Standard Template Library (STL) provides container classes that offer programmers the functionality found in classic data structures like arrays, lists and queues, without having to reinvent the wheel. I'll devote a future article to the use of the STL but in this example, Weapons Array is a class that inherits the functionality of the vector<Item> container class that is instantiated with pointers to Weapon(s). This is what the Weapon * symbolizes in the solid box adorning the Weapons Array class.

Figure 1 also shows that Submarine and Surface Ship inherit the characteristics of Vessel. Steam Plant, Gas Turbine Plant and Nuke Plant inherit Plant's characteristics and Close In Weapon System (CIWS), Five Inch Gun and Torpedo inherit from Weapon. Remember, these are classes, not objects. When it comes time to construct the fleet, you can make as many different objects of each class as are required.

Now, to tie all the elements of Figure 1 together, a Vessel has a Plant and a Weapons Array. A Weapons Array will be loaded with various types of Weapons. The key to understanding polymorphic behavior lies in understanding that where ever you use a Weapon, you can use a CIWS, Five Inch Gun or a Torpedo derived class object (Or other classes derived from Weapon). And, where ever you use a Plant, you can also use a Steam Plant, Gas Turbine Plant or Nuke Plant object. The same holds for Vessel and any classes derived from Vessel.

Figure 2 on page 33 is a dynamic diagram that shows the interaction among the fleet objects. When a Vessel receives an order to light off its engineering plant, the Vessel, in turn, sends a light off order to its Plant in the form of the LightOff_Plant() method. When the plant object receives the LightOff_Plant() command it returns plant status. The other methods associated with command and control of the computer-controlled fleet are read in similar fashion.

The complete source code listing for the computer-controlled fleet is too long to include in its entirety, but I'd like to highlight a few points.

The abstract base class Vessel is declared in the header file vessel.h as follows:

```
#ifndef MY_VESSEL_H
#define MY_VESSEL_H
#include <vector.h>

class Plant;
class Weapon;
class Vessel
{
public:
 Vessel(Plant &thePlant, vector<Weapon*> &theWeapon_Array);
  virtual ~Vessel();
  virtual void LightOff_Plant() = 0;
  virtual void ShutDown_Plant() = 0;
  virtual void Train_Weapon() = 0;
  virtual void Fire_Weapon() = 0;
  virtual bool Get_Plant_Status() = 0;

protected:
  Plant &GetPlant() {return itsPlant;}
      vector<Weapon*>   &GetWeapon_Array()   {return
itsWeapon_Array;}

private:
  Plant &itsPlant;
  vector<Weapon*> &itsWeapon_Array;
  static int count;
};
#endif
```

Notice that with the exception of the constructor and destructor, the interface methods are declared as pure virtual functions. This is achieved by setting the function to equal zero. When a function is declared as pure virtual it will NOT be defined in the base class, but must be defined later in a derived class.

Having said that, let's take a look at the Submarine class declaration which appears in the header file submarine.h:

```
#ifndef MY_SUBMARINE_H
#define MY_SUBMARINE_H

#include "vessel.h"
#include <vector.h>

class Submarine : public Vessel
{
public:
            Submarine(Plant&thePlant,vector<Weapon*>
&theWeapon_Array, char *theName);
  virtual ~Submarine();
  virtual void LightOff_Plant();
  virtual void ShutDown_Plant();
  virtual void Train_Weapon();
  virtual void Fire_Weapon();
  virtual bool Get_Plant_Status();

private:
  char *itsName;
  static int count;
};
#endif
```

Notice here that the interface functions LightOff_Plant(), ShutDown_Plant(), etc., are not set to equal zero; therefore, they must be defined. *Submarine's interface functions are defined in the implementation file submarine.cpp as follows:*

```
#include “submarine.h”
#include <iostream.h>
#include “plant.h”
#include “weapon.h”
#include <vector.h>

int Submarine::count = 0;

Submarine::Submarine(Plant &thePlant, vector<Weapon*> &theWeapon_Array, char *theName): Vessel(thePlant, theWeapon_Array), itsName(theName)
{
  if((++Submarine::count) == 1)
      cout<<“Constructor: There is “<<Submarine::count<<“ submarine.”<<endl;
    else
      cout<<“Constructor: There are “<<Submarine::count<<“ submarines.”<<endl;
}

Submarine::~Submarine()
{
  if((—Submarine::count) == 1)
      cout<<“Destructor: There is “<<Submarine::count<<“ submarine.”<<endl;
    else
      cout<<“Destructor: There are “<<Submarine::count<<“ submarines.”<<endl;
}

void Submarine::LightOff_Plant()
{
  GetPlant().LightOff_Plant();
}

void Submarine::ShutDown_Plant()
{
  GetPlant().ShutDown_Plant();
}

void Submarine::Train_Weapon()
{
  vector<Weapon*>::iterator i;
 for(i=GetWeapon_Array().begin(); i != GetWeapon_Array().end(); i++)
    (*i)->Train_Weapon();
}

void Submarine::Fire_Weapon()
{
  vector<Weapon*>::iterator i;
 for(i=GetWeapon_Array().begin(); i != GetWeapon_Array().end(); i++)
    (*i)->Fire_Weapon();
}

bool Submarine::Get_Plant_Status()
{
  return GetPlant().Get_Plant_Status();
}
```

Let's examine Submarine's Train_Weapon() function. If you're not used to seeing STL code, the syntax will seem foreign. The important point here is that a Submarine object will access its weapons through its Weapons Array. It has no knowledge of the exact weapon objects contained in the array, nor does it know how many weapons are contained in the array. All Submarine knows (i.e., the designer of Submarine functions) is that a Weapons Array object can be manipulated through the interface provided for in the vector<Weapon*> parameterized class. Through the use of iterators, and STL programming idioms, designers can train (and fire) the weapons in Submarine's Weapon Array without concern for the nasty details. This is generic programming and an example of polymorphic behavior.

Now, lets build a small fleet of vessels with different engineering plants and weapon systems and exercise their capabilities. *The code that accomplishes this is located in the main() function in file main.cpp:*

```
#include <iostream>
#include “vessel.h”
#include “submarine.h”
#include “Surface_Ship.h”
#include “weapon.h”
#include “ciws.h”
#include “torpedo.h”
#include “five_inch.h”
#include “plant.h”
#include “nuke_plant.h”
#include “steam_plant.h”
#include “gasturbine_plant.h”
#include <vector.h>


int main()
{
/*****************************
  Make an array of base class
  pointers
*****************************/

 Vessel *myNavy[3];

/*****************************
  Make some plants to power
  the vessels...
*****************************/
```

►

```
Nuke_Plant        Nuke1("Liquid Metal");
Steam_Plant       Steam1(1200);
GasTurbine_Plant  GasTurbine1("LM5000");

/*****************************
  Make some weapons...
*****************************/

Ciws      Ciws1("MK1001", 5000);
Ciws      Ciws2("MK1001", 5000);
Ciws      Ciws3("MK1001", 5000);
Ciws      Ciws4("MK1001", 5000);

Five_Inch  FiveInch1("Super Shot", 400);
Five_Inch  FiveInch2("Super Shot", 400);


Torpedo    Torpedo1("MK87", 25);
Torpedo    Torpedo2("MK87", 25);
Torpedo    Torpedo3("MK87", 25);

/******************************
   Declare three vectors of Weapon
   pointers.
******************************/
  vector<Weapon*> WepArray1(3);
  vector<Weapon*> WepArray2(3);
  vector<Weapon*> WepArray3(3);

/*******************************
  Load weapon arrays with addresses
  of derived weapon objects...
*******************************/

WepArray1[0] =  &Ciws1;
WepArray1[1] =  &Ciws2;
WepArray1[2] =  &FiveInch1;

WepArray2[0] = &Ciws3;
WepArray2[1] = &Ciws4;
WepArray2[2] = &FiveInch2;

WepArray3[0] = &Torpedo1;
WepArray3[1] = &Torpedo2;
WepArray3[2] = &Torpedo3;

/*****************************
  Construct various vessels...
*****************************/

Submarine      Sub1(Nuke1, WepArray3, "SSN 714");

Surface_Ship   Ship1(Steam1, WepArray1, "Skimmer");
Surface_Ship   Ship2(GasTurbine1, WepArray2, "Skimmer2");

/********************************
  load fleet array with addresses
  of derived vessel objects
********************************/

myNavy[0] = &Sub1;
myNavy[1] = &Ship1;
myNavy[2] = &Ship2;

/*********************************
  call polymorphic functions
*********************************/

  for(int i = 0; i<3; i++)
  {
    myNavy[i]->LightOff_Plant();
    myNavy[i]->Train_Weapon();
    myNavy[i]->Fire_Weapon();
    myNavy[i]->ShutDown_Plant();
  }
 return 0;
}
```

Notice there are no Vessel objects. myNavy is an array of Vessel base class pointers, which is allowed. There are also no Weapon or Plant objects — only objects of classes derived from Weapon or Plant.

Polymorphic programming is a tricky concept to master. Once you understand how to implement polymorphic behavior in code, your object-oriented solutions will become both increasingly generic and robust. This is a tremendous aid to code reuse and maintenance.

The complete source code for the Fleet Simulator can be obtained via the internet at www.warrenworks.com. Follow the link to the C++ resource page.

References

Booch, Grady. "Object-Oriented Analysis and Design with Applications", 2nd Edition. Benjamin/Cummings Publishing Company, Inc. Redwood City, CA. 1994.

Sadar, Babak. "Unified Objects: Object-Oriented Programming Using C++", IEEE Computer Society Press, Los Alamitos, CA. 1998

About the Author: LT Miller is the Software Division Officer at Naval Medical Center San Diego and serves as an adjunct faculty member at Southwestern College and National University. He can be reached at millerrw@acm.org.

Now Enrolling:

Managing Information Technology Programs and Acquisitions

NCTS Pensacola is offering this course to help students understand and apply the objectives of current DoD Information Technology (IT) Program and Acquisition policies.

Lessons are based upon DoD 5000.2-R, Mandatory Procedures for Major Defense Acquisition Programs (MDAPs) and Major Automated Information System (MAIS) Acquisition Programs and references, Information Technology (IT) Investment Management Insight Policy for Acquisition and various Abbreviated Acquisition Program procedures unique to the Departments of the Navy, Marine Corps, Air Force and Army.

Past Life Cycle Management (LCM) requirements are briefly discussed to help students grasp fundamental policy changes resulting from Acquisition Reform such as new terms and definitions, life cycle phase requirements, approval thresholds, roles and responsibilities of key players, and milestone decision point expectations. Cultural changes including insight versus oversight and the distinction between mandatory and discretionary procedures, information and documentation are explored.

Workshops are provided to help students adapt the intent of current policies to IT programs and acquisitions in which they are involved. Various information sources and automated tools are also suggested to provide students additional assistance upon completion of this training.

TARGET AUDIENCE: Attendees of previous NCTS Pensacola LCM courses, MDAs, PMs, IPT members and PM staff, i.e., procurement, budget, functional personnel (analysts and end users) and technical personnel (computer, telecommunications, security and test and evaluation specialists, design analysts, developers and operations managers) relative to major and less than major IT programs.

TUITION: $500 per person (first time enrollment) or $400 per person (previous attendee of any NCTS Pensacola LCM course) or $300 per person (group enrollment of 3 or more). There is a 20 student minimum and a 30 student maximum requirement per class.

Cost reduced
$100 per student

FY98 TRAINING SCHEDULE

1-3 April	Norfolk, VA
7-9 April	Cherry Point, NC
21-23 April	San Diego, CA
5-7 May	Washington, DC
20-22 May	Honolulu, HI
2-4 June	New Orleans, LA
7-9 July	San Antonio, TX
4-6 August	Memphis, TN
8-10 Sept	Pensacola, FL

FOR ADDITIONAL COURSE INFORMATION AND ENROLLMENT ASSISTANCE:

PHONE:	DSN 922-3501 Commercial (850) 452-3501
FAX:	(850) 452-8701
INSTRUCTORS:	Kelley Harris (ext. 612) Van Kirkland (ext. 104) Paul Love (ext. 636)

THIS COURSE CAN BE SCHEDULED ONSITE AND TAILORED TO MEET YOUR SPECIFIC TRAINING REQUIREMENTS. IF INTERESTED, PLEASE CONTACT:

Alice Brown, N83 Division Director at ext. 701 or FAX (850) 452-9120. You may also send email inquiries to alice.brown@ncts.navy.mil or write to:

Commanding Officer
Naval Computer and Telecommunications Station
130 West Avenue Suite B
Pensacola, FL 32508-5111
Attn: N83

Color Printing continued from page 32

conductive belt. A laser beam exposes the areas *not* to be printed, leaving charged the areas that *will* be printed. Powdered toner sticks to the charged areas of the drum. The image on the drum is transferred to another belt and then to the paper. Finally, the image is fused to the page with heat and pressure.

Color laser printers such as the Tektronix Phaser 560 produce images up to 1200 X 1200 dpi. Some laser printers use interpolation or resolution enhancement to achieve a higher output resolution. This method may increase print times and not provide the desired quality. This technology also requires a complex printing mechanism and consumable components that must be replaced when empty or worn out.

Color laser technology can also be used to print black and white documents using shades of gray for quality output at a low cost. Color letterhead at a resolution of 600 dpi can be printed and then reprinted on a faster black and white laser. In our office test, we discovered that printing above 600 dpi caused the colored letterhead's image to be duplicated across the drum of the black and white printer, which could lead to printer damage.

Solid ink printers such as the Tektronix Phaser 340 or 350 can produce sharp color output. This type of printer uses solid ink sticks inserted into the print head where they are melted. The ink is then sprayed onto the paper where it solidifies. Each ink storage holder is a distinct shape, which makes it almost impossible to load the ink blocks incorrectly.

We tested the Tektronix Phaser 340 and 350 and discovered that even though the printer was noisy and slow (4-6 pages per minute), it printed Pantone colors with no adjustments necessary. The color was sharp and large graphics printed at standard speed. This technology produces high color at a low cost, especially since Tektronix is giving free black ink for the Phaser 340 or 350. Different weight paper can be used with the solid ink printers.

However, this technology can't be used for printing colored letterhead with the anticipation of using a black and white laser for the body of the document. Since the solid ink is melted on, it will become soft when the document is put through another laser printer. The ink will stick to the drum of the black and white laser causing significant damage.

The solid ink technology is easy to use and costs less than toner.

Thermal wax or transfer printers produce high quality output by melting wax from ribbons and applying the wax to a page. Typically these printers use either a three-color ribbon (cyan, magenta and yellow) or four colors with black. As with any printer, the more colors used, the sharper the output. The thermal print head consists of tiny elements that are heated to melt dots of color onto paper or transparencies. The paper makes three or four passes under the print head using a half-toning process similar to the colored dot printing used in newspapers to achieve the effect of millions of colors. The more passes, the better the quality.

These printers work well with transparencies and create vibrant color presentations. This technology is similar to the solid ink printers – they print slowly with long waits to warm up the print head.

These printers typically require a special coated paper to obtain high-quality images and are more expensive than solid ink printers. However, they are ideally suited for printing with a maximum amount of colors.

Dye Sublimation is the last type of color printer we'll talk about. These printers produce near-photographic quality output. They use a technology similar to thermal printers, but rather than use a transfer roll with pigments in wax, they use dye sublimation (also referred to as dye diffusion). These rolls contain solid dyes with either three or four colors. This technology is typically used to create proofs or graphic designs. Obviously, these printers are quite expensive, costing over $5K.

These printers best fit a market of specialty applications that require photographic quality.

What does DPI mean and how much do I need?

Dpi stands for dots per inch, with the highest resolution having the most dots. With color printers, dpi is not always a good measuring tool. The process by which the colors are created can affect the quality of output.

Color printers create color by mixing black, cyan, magenta and yellow. The colored dots are placed closely together to produce the desired color. Continuous tone printing combines the colors in varying amounts on top of each other to produce a visual impression of a single color.

Dithered images need more dots or a greater resolution to create the same quality of image. Dithering printers typically offer resolutions of 600 to 1200 dpi.

Resolution is also affected by the technology. Check to see if the printer's output resolution is interpolated, resolution enhanced via software or firmware or whether the print engine is a true dpi as stated. The method the color printer uses can hamper the printing speed.

How many people will use the color printer?

Since some technologies are slower than others, you'll want to decide how many people will be using the printer and what type of documents they'll be printing.

Ink jets are great for personal desktops or small work groups of 2-5 people. They allow the user to produce low cost, quality prints.

Color laser printers are good for volume output for large work groups or LANs. Since color laser printers vary in speed, be sure to select a printer that won't bottleneck production. Color laser printers such as the HP Color LaserJet or the Tektronix Phaser have the capability of directly connecting to the network.

Tektronix offers a product called Phaser Share with each printer having its own web page, if you have an available Internet Protocol (IP) address. This allows the administrator to change printer settings, check on status of print jobs or control printed output via a network node or remotely via the Internet. HP offers its JetDirect manager for directly connected color printers.

Laser printers are quieter than solid ink printers and print documents faster. Be sure to select a printer that offers different print modes such as 600 dpi, 1200 dpi, draft, economy, etc. which allows the end-user to select the desired quality.

Will the printed color documents pass through many hands?

Typically, high resolution printed documents take a little time to dry, so try not to place your hands on a printed sheet as soon as it comes out of the printer. Solid ink and wax printers melt a colored solution on to the page, which at times may be scratched off or smeared.

Color laser printers are tougher, since the color output is a dry toner-based product. Check for printers that provide a matte finish.

If the printed documents are going to have very little handling or the user can wait a few moments to let the paper dry, the other technologies which provide bright colors can be used.

Will you need to make copies of the color originals?

This is an easy question – of course you will. Using a technology that offers a low per-page cost lets you print multiple copies economically. Since color copiers are expensive, using a color printer is a viable option.

We used our color laser and solid ink printers to produce the materials for our last two Department of the Navy Connecting Technology conferences.

Look for the hidden operation costs.

Each technology has a different cost per page with the ink jets, lasers and solid ink printers using standard bond or 20 lb. copier paper. The dye sublimation uses a high cost paper. Check the printer specifications on the cost per page prior to saying *yes.*

Set an office policy for color printing. For example, is there really a need to print e-mail messages in color? Even though the printers we've mentioned print on standard paper, except for the dye sublimation printers, a special paper may have to be purchased for a particular result. Photo quality ink jet paper can cost $1 per page or more.

Will you need black and white documents in addition to color?

Most documents created in an office are black and white, so the printer's speed for printing black and white text is important. For the most part, print speed for ink jets and solid ink printers does not change with black only text. With color laser printers, the speed change can be significant.

Dye sublimation printers would be wasted on black and white documents. A color printer for printing black and white documents is a consideration, especially if the black ink is free and time isn't an issue.

What paper size is needed?

Virtually, all color printers handle 8.5" x 11" paper, but what if you need something larger such as 8.5" x 14" or 11" x 17"? Some ink jets handle a variety of envelopes, banners, up to 11" x 17" sheets, or even T-shirt transparencies. Some other color printers can handle large sheets by using rolls of paper or film. Paper rolls are mostly associated with dye sublimation or thermal wax printers for producing large color prints. Laser printers typically output standard and legal size documents.

Various color printers may require special add on components for different paper sizes, manual feed or card stock.

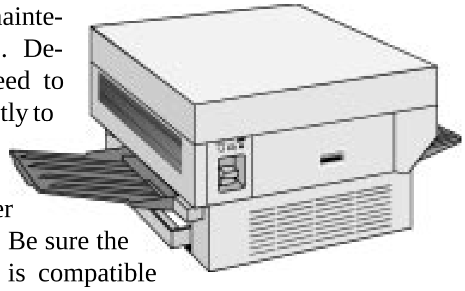
The Tektronix Phaser 560 lets you place multiple sheets of legal size paper, card stock, business card paper or envelopes in the built-in tray.

Pricing?

There are color printers available through the Navy's IDIQ contracts and blanket purchase agreements (BPAs). Check the prices listed by viewing our web page at http://www.chips.navy.mil/it.

Buying tips.

Consider the cost of maintenance and consumables. Decide whether you'll need to connect the printer directly to your network, remotely administer the printer(s) or easily setup the driver for each network node. Be sure the printer's network card is compatible with your network operating system.



About the Author: Koehler is a Computer Specialist at NCTAMS LANT. He manages the ULANA II and SBIS contracts for the Navy. He can be reached via email at patrick_koehler@ccmail.nctamslant.navy.mil.

Under the Contract

ViViD - Lucent
N6839-97-D-0040

Mod 5 added information regarding the contract usage fee. All CLIN/SLIN prices in this contract include the fee which supports the Navy Umbrella Contracts Program. This fee allows the contract sponsor, SPAWAR, to recover the expenses of awarding and managing this and other contracts. The application and amount of this fee, as included in the contract unit prices, are at the sole discretion of the Navy and are not subject to dispute.

Mod 6 added instructions for the Coast Guard. For information concerning the contract and ordering, Coast Guard should contact:

Technical Specifications and Support Branch
Code N811.2
NCTAMS LANT
9625 Moffett Ave.
Norfolk, VA 23511-2784
COMM: (757) 445-1493
FAX: (757) 445-2103
DSN: 565-XXXX

The payment office for the Coast Guard is:
Commanding Officer
USCG Finance Center
1430A Kristina Way
Chesapeake, VA 23326

Mod 7 effective 12 January 98 changed the accounting information for the minimum guarantee and appropriation data.

Mod 8 effective 21 January 98 provides pricing for bulk purchase of certain cable CLINs. Please reference the CLIN list below for the new pricing information. These changes replaced exhibit A3.

SLIN	DESCRIPTION	PRICE
0327AA	Shipboard 8 Fiber Cable, MM-Bulk Thermoset, Brand-Rex, OC1434, Minimum Order 2,000 Ft	$6.51/ft
0328AA	Shipboard 8 Fiber Cable, MM-Bulk Thermoplastic, Brand-Rex, M85045/13-0, Minimum Order 2,000 Ft	5.10/ft
0329AA	Shipboard 4 Fiber Cable, MM-Bulk Thermoset, Brand-Rex, OC1417, Minimum Order 2,000 Ft	4.70/ft
0329AB	Shipboard 4 Fiber Cable, MM-Bulk Thermoset, Brand-Rex, OC1417, Minimum Order 50,000 Ft	4.50/ft
0329AC	Shipboard 4 Fiber Cable, MM-Bulk Thermoset, Brand-Rex,OC1417, Minimum Order 100,000 Ft	4.30/ft
0329AD	Shipboard 4 Fiber Cable, MM-Bulk Thermoset, Brand-Rex, OC1417, Minimum Order 150,000 Ft	4.10/ft
0330AA	Shipboard 4 Fiber Cable, MM-Bulk Thermoplastic, Brand-Rex, M85045/15-01, Minimum Order 2,000 Ft	3.10/ft
0330AB	Shipboard 4 Fiber Cable, MM-Bulk Thermoplastic, Brand-Rex, M85045/15-01, Minimum Order 10,000 Ft	2.74/ft

Mod 9 added several technology enhancement CLINs and changed the Contract Order Management point of contact. The point of contact is now Elaine McDaniel. She can be reached at (757) 445-1493; DSN 565. Her e-mail address is erroneous in the modification. The correct e-mail is elaine_mcdaniel@ccmail.nctamslant.navy.mil. Please use the underscore in lieu of the period between elaine and mcdaniel.

Additionally, when ordering installation services please include a copy of the hardware and software CLINs with the installation delivery order. Under this modification CLIN 1012AA was added to provide Lucent Products from their GSA schedule. These products are discounted by 0.9 percent from the GSA price. A list of products can be downloaded from the Umbrella Program web site located at www.chips.navy.mil/it. You can download the GSA schedule as file 1012AA or the entire contract.

NCTAMS LANT Point of Contact
Technical Specifications and Support Branch

Tech Support:	Lisa Hunt (757) 445-2568; DSN 565
E-mail:	lisa_hunt@ccmail.nctamslant.navy.mil
Fax:	(757) 445-2103; DSN 565
Web Site:	www.chips.navy.mil/it/contract/vivid-lucent.html

ViViD - GTE
(N68939-97-D-0041)

Mod 5 (P00005 signed November 26, 1997) contains:

- New SCLINS for the FORE ASX-1000 ATM switch and related components.
- New SCLINS for the ForeThought ATM Internetworking Software and Networking Management Software.
- New SCLINS for tight buffered fiber optic cabling, ST connectors, and misc components for pier side connectivity.
- Price reductions for some of the ASX200BX software products.
- Unit of issue changes on cables, CLINs 0200-0204, changed from 250 FT. COIL to 100 FT. COIL.

Mod 6 (P00006 signed December 23 1997) contains:

- Administrative changes to Section G and Exhibit A3 which includes address and payment office.
- Changes to A1E and A2E which include Description/Part Number changes as made to CLIN 4725AA/5025AA/ 5325AA/6400BL.

Mod 7 (P00007 signed January 12, 1998) contains:

- Administrative changes to Section G to change the Minimum Guarantee Accounting and Appropriation Data. You may update your contract files by downloading and substituting sections A1E, A2E, A3 and G located at the Navy IT web page: http://www.chips.navy.mil/it

NCTAMS LANT Point of Contact
Technical Specifications and Support Branch

Tech Support:	Rick Paquin (757) 445-2568; DSN 565
E-mail:	rick_paquin@ccmail.nctamslant.navy.mil
Fax:	(757) 445-2103; DSN 565
Web Site:	www.chips.navy.mil/it/contract/vivid-gte.html

Government POCs

Program Manager:	Nikki Isfahani
COMO POC:	Jackie Smith
Deputy Program Manager:	David Mullins
NCTAMS LANT Network Testing & Product Configuration Manager:	Rick Paquin

PCLAN Plus
(N68939-95-D 0018)

CLINs and prices are based on **Mod 26** (1 Feb 98), **Mod 27** (1 Feb 98) and **Mod 28** (11 Feb 98). Items can be ordered through 31 Jan 2001.

Mod 28 CLINs 0101AR and 0101BE (Micronics IT21 Workstations with 1 year spare-in-the-air warranty) have been suspended from ordering on the contract. *The following CLINs have been updated from Pentium Pro to Pentium II technology:*

CLIN	DESCRIPTION	PRICE
0101AM	Micronics IT21 Workstation, 100Base TX, with the following: Micronics Intel Pentium II 233/512KB Cache CPU, Minitower ATX Case Three 5.25" ext bays; two 3.5" ext bays; one 3.5" int bay 3.2GB EIDE Hard Drive 64MB SDRAM 24X CD ROM drive Dual slot PCMCIA Card Reader Dual USB Ports Keyboard, MS Mouse and mouse pad 3.5" FDD 17-inch color monitor PCI Video Card w/2MB RAM, SoundBlaster 16-Bit compatible sound system w/amplified 14 watt speakers. PCI 10/100 Fast Ethernet UTP-5 NIC NT Workstation 4.0 with Service Pack 3	$2,576
0101BA	Micronics IT21 Workstation, 100Base FX, with the following: Micronics Intel Pentium II 233/512KB Cache CPU, Minitower ATX Case Three 5.25" ext bays; two 3.5" ext bays one 3.5" int bay, 3.2GB EIDE Hard Drive 64MB SDRAM, 24X CD ROM drive Dual slot PCMCIA Card Reader Dual USB Ports, Keyboard, MS Mouse and mouse pad , 3.5" FDD 17-inch color monitor PCI Video w/2MB RAM SoundBlaster 16-Bit compatible sound system w/ amplified 14 watt speakers PCI 100BaseFX ST NIC NT Workstation 4.0 with Service Pack 3	2,817
0101CH	Micronics IT21 Workstation, 100Base FX, with the following: Micronics Intel Pentium II 233/512KB Cache CPU, Desktop ATX Case Two 5.25" ext bays; two 3.5" ext bays one 3.5" int bay, 3.2GB EIDE Hard Drive 64MB SDRAM, 24X CD ROM drive Dual slot PCMCIA Card Reader Dual USB Ports, Keyboard, MS Mouse a and mouse pad, 3.5" FDD 17-inch color monitor PCI Video w/2MB RAM SoundBlaster 16-Bit compatible sound system w/ amplified 14 watt speakers PCI 100BaseFX ST NIC NT Workstation 4.0 with Service Pack 3	2,817

The following Pentium II technology CLINs and associated CLINs have been added to the contract:

CLIN	DESCRIPTION	PRICE
0101AV	Micronics IT21 Workstation, 100Base TX, with the following: Micronics Intel Pentium II 233/512KB Cache CPU, Desktop ATX Case Two 5.25" ext bays; two 3.5" ext bays one 3.5" int bay 3.2GB EIDE Hard Drive 64MB SDRAM, 24X CD ROM drive Dual slot PCMCIA Card Reader Dual USB Ports, Keyboard, MS Mouse and mouse pad 3.5" FDD, 17-inch color monitor PCI Video w/2MB RAM SoundBlaster 16-Bit compatible sound system w/ amplified 14 watt speakers PCI 10/100 Fast Ethernet UTP-5 NIC NT Workstation 4.0 with Service Pack 3	$2,576
0101CK	IT21 Workstation Software Bundle is available when purchased with CLINs 0101AM, 0101AV, 0101BA, or 0101CH Office Professional 97 WinZip 6.3 SR-1 (or later) Netscape Communicator Pro BackOffice Client Access License	615
0106Ax	Trandmark Pentium II configurable bundle standard features: Intel Pentium II CPU with 512KB L2 cache Motherboard with Intel 440LX chipset 32MB SDRAM memory 2.5GB EIDE Hard Disk Drive AGP 3D Video card with 4Mb Video Ram 24X CD ROM drive Dual slot PCMCIA Card Reader 3.5" FDD Six expansion slots: 1 shared ISA/PCI slot (ISA slot used for sound), 1 ISA slots (used for PCMCIA), 4 PCI slots (3 open) 1 AGP slot (used for video) 2 Serial ports, 16550 compatible 1 ECP/EPP parallel port Mode 4 Enhanced IDE Ultra DMA/33 2 standard 40-pin IDE connectors 1 standard floppy disk connector 2 USB ports SoundBlaster 16-Bit compatible sound system w/ amplified 14 watt speakers Desktop ATX case: two 5.25" external bays; two 3.5" external bays 200 watt power supply OR Mini Tower ATX case; three 5.25"external bays; two 3.5" external bays, 200 watt power supply	

▶

CLIN	DESCRIPTION	PRICE
	Battery powered real-time clock/calendar; front panel LEDs Enhanced 104 keyboard; 2 Button mouse mouse pad, power cord	

CLINs that can be integrated with configurable Pentium II bundles CLIN 0106AA through 0106AH:

0100TN - 0100TP	Separately orderable EIDE hard drives
0101AF	Fast Ethernet Fiber NIC, ST Connector
0101AG	Fast Ethernet Fiber NIC, SC Connector
0041AB	PCI fast Ethernet Network card (RJ-45)
0100TY	MS Office 97 Single User License & CD
0106BA	MS NT Workstation 4.0
0106BB	MS Windows 95
0106CA	32 MB SDRAM DIMM
0106CB	64 MB SDRAM DIMM
0106CC	128 MB SDRAM DIMM
0200BA, 0290CA, 0291AA	Color monitors 15", 17" or 21"

CLIN	DESCRIPTION	PRICE
0106AA	Pentium II 233 Desktop configurable bundle (CLIN 0106Ax), includes: Intel Pentium II 233MHz CPU with 512KB cache, AGP Video w/4MB RAM	$1,439
0106AB	Pentium II 233 tower configurable bundle (CLIN 0106Ax), includes: Intel Pentium II 233MHz CPU with 512KB cache, AGP Video w/4MB RAM	1,439
0106AC	Pentium II 266 Desktop configurable bundle (CLIN 0106Ax), includes: Intel Pentium II 266MHz CPU with 512KB cache, AGP Video w/4MB RAM	1,567
0106AD	Pentium II 266 tower configurable bundle (CLIN 0106Ax), includes: Intel Pentium II 266MHz CPU with 512KB cache, AGP Video w/4MB RAM	1,567
0106AE	Pentium II 300 Desktop configurable bundle (CLIN 0106Ax) includes: Intel Pentium II 266MHz CPU with 512KB cache, AGP Video w/4MB RAM	1,899
0106AF	Pentium II 300 tower configurable bundle (CLIN 0106Ax), includes : Intel Pentium II 266MHz CPU with 512KB cache, AGP Video w/4MB RAM	1,899
0106AG	Pentium II 333 Desktop configurable bundle (CLIN 0106Ax) includes: Intel Pentium II 266MHz CPU with 512KB cache, AGP Video w/4MB RAM	2,155
0106AH	Pentium II 333 tower configurable bundle (CLIN 0106Ax), includes: Intel Pentium II 266MHz CPU with 512KB cache, AGP Video w/4MB RAM	2,155
0106BA	Microsoft NT Workstation 4.0 to be integrated in any of the following CLINS: 0106AA, 0106AB, 0106AC, 0106AD, 0106AE, 0106AF, 0106AG, 0106AH	199
0106BB	Microsoft Windows 95 to be integrated in any of the following CLINS: 0106AA, 0106AB, 0106AC, 0106AD, 0106AE, 0106AF, 0106AG, 0106AH	118
0106CA	32MB SDRAM DIMM 64 Bit/66MHz Pentium II Memory expansion consisting of one 32MB DIMM strip to be integrated in any of the following CLINS: 0101AM, 0101AR, 0101AV, 0101BA, 0101BE, 0101CH, 0106AA, 0106AB, 0106AC, 0106AD, 0106AE, 0106AF, 0106AG, 0106AH	145
0106CB	64MB SDRAM DIMM 64 Bit/66MHz Pentium II Memory expansion consisting of one 64MB DIMM strip to be integrated in any of the following CLINS: 0101AM, 0101AR, 0101AV, 0101BA, 0101BE, 0101CH, 0106AA, 0106AB, 0106AC, 0106AD, 0106AE, 0106AF, 0106AG, 0106AH	324
0106CC	128MB SDRAM DIMM 64 Bit/66MHz Pentium II Memory expansion consisting of one 128MB DIMM strip to be integrated in any of the following CLINS: 0101AM, 0101AR, 0101AV, 0101BA, 0101BE, 0101CH, 0106AA, 0106AB, 0106AC, 0106AD, 0106AE, 0106AF, 0106AG, 0106AH	825

The prices have been decreased on the following CLINs:

CLIN	DESCRIPTION	PRICE
0100TB	Micronics Pentium P166 Desktop Server/Workstation	$1,160
0100TC	Micronics Pentium P200 Desktop Server/Workstation	1,202
0100TE	Micronics Pentium P166 Mini Tower Server/Workstation	1,171
0100TF	Micronics Pentium P200 Mini Tower Server/Workstation	1,213

The following CLINs have been deleted from the contract:

CLIN	DESCRIPTION
0100BA-BC	Compaq - ProSignia 200
0101AA-AC	Micronics Pentium Pro Workstation Bundle
0101AN-AQ	Micronics IT21 Pentium Pro Workstation
0101AS-AU	Micronics IT21 Pentium Pro Workstation
0101BB-BD	Micronics IT21 Pentium Pro Workstation
0101BF-BH	Micronics IT21 Pentium Pro Workstation
0201AA	Compaq P6/166 ProLiant 5000 Advanced Server
0201AB	Compaq P6/166 ProLiant 5000 Array Server
0201AF	Compaq SMART 2/E SCSI Array Controller for EISA Bus
0201AG	Compaq ProLiant Storage System Model 1
0202AD	Rack Mounted Compaq ProLiant Storage System Model 1

Mod 27 extends the PCLAN+ contract into year 3.
Mod 26 Microsoft Exchange Enterprise Server and Client Licenses have been updated to version 5.5 (CLINs 1140HA-HH).

Microsoft Front Page 97 has been updated to Microsoft Front Page 98 (CLINs 1132AA-AG).

The Cisco Products, CLIN 0015AA, has been released from Y2K supension. However, **only** Year 2000 compliant products can be purchased. Please check the web site www.cisco.com/warp/public/752/2000/cptbl_ov.htm for a list of compliant products.

The Sidewinder Firewall software (CLIN 0019xx) has been upgraded to version 3.2.

The prices have been decreased on the following CLINs:

CLIN	DESCRIPTION	PRICE
0013CA	Cabletron - F7069 and F7069-DAS; 32-bit FDDI EISA DAS NIC	$1,725
0013CB	Rockwell - RNS-2200-FD, PCI Bus FDDI DAS NIC	1,283
0024BA	SMC9746F ATM Power 155 PCI Server Adapter with 2MB RAM and SC-type MMF interface	1,273
0100BD	16MB Memory Expansion for ProSignia 200	109
0100BE	32MB Memory Expansion for ProSignia 200	185
0100BF	64MB Memory Expansion for ProSignia 200	392
0100EA	8MB SIMM 32 Bit/70ns expansion for LES/W	54
0100EB	16MB(2x8MB SIMMs) 36 Bit/70ns ECC Memory expansion kit for MS/W	152
0100ED	16MB EDO memory expansion for Micronics Pentium Server/Workstation (2x8MB strips, 32 Bit/70ns)	109
0100EE	32MB EDO memory expansion for Micronics Pentium Server/Workstation (2x16MB strips, 32 Bit/70ns)	196
0100EF	64MB EDO memory expansion for Micronics Pentium Server/Workstation (2x32MB strips, 32 Bit/70ns)	370
0100EG	8MB ECC memory for ProSignia 300 (2x4MB strips, 36 Bit/70ns)	76
0100EH	16MB ECC memory for ProSignia 300 (2x8MB strips, 36 Bit/70ns)	152
0100EJ	32MB ECC memory for ProSignia 300 (2x16MB strips, 36 Bit/70ns)	239
0100EK	64MB ECC memory for ProSignia 300 (2x16MB strips, 36 Bit/70ns)	458
0100EL	8MB ECC memory for ProLiant 1500 (2x4MB strips, 36 bit/60ns)	76
0100EM	16MB ECC memory for ProLiant 1500 (2x8MB strips, 36 bit/60ns)	152
0100EN	32MB ECC memory for ProLiant 1500 (2x16MB strips, 36 bit/60ns)	239
0100EP	64MB ECC memory for ProLiant 1500 (2x32MB strips, 36 bit/60ns)	458
0100EQ	16MB ECC memory for ProLiant 4500 (4x4MB strips, 36 bit/70ns)	152
0100ER	32MB ECC memory for ProLiant 4500 (4x8MB strips, 36 bit/70ns)	283
0100ES	64MB ECC memory for ProLiant 4500 (4x16MB strips, 36 bit/70ns)	458
0100ET	128MB ECC memory for ProLiant 4500 (4x32MB strips, 36 bit/70ns)	916
0100EU	256MB ECC memory for ProLiant 4500 (4x64MB strips, 36 bit/70ns)	1,832
0100EV	16MB ECC memory for ProLiant 800 (60ns, EDO, ECC RAM)	130
0100EW	32MB ECC memory for ProLiant 800 (60ns, EDO, ECC RAM)	299
0100EX	64MB ECC memory for ProLiant 800 (60ns, EDO, ECC RAM)	539
0101AH	3.8GB EIDE Hard Disk Drive, separately orderable	300
0105BA	Compaq Armada Laptop Memory 8 MB Upgrade Kit	70
0105BB	Compaq Armada Laptop Memory 16 MB Upgrade Kit	125
0105BC	Compaq Armada Laptop Memory 32 MB Upgrade Kit	234
0105EA	3COM EtherLink III LAN and 33.6 Modem PCMCIA Card	320
0201AD	Compaq ProLiant 5000 Pentium Pro 166/512 CPU (For adding CPUs 2, 3, 4 to the ProLiant 5000)	1,831
0201AM	64MB Memory Expansion Kit (4x16MB DIMMs) for ProLiant 5000	567
0201AN	128MB Memory Expansion Kit (4x32MB DIMMs) for ProLiant 5000	1,058
0201AQ	512MB Memory Expansion Kit (4x128MB DIMMs) for ProLiant 5000	5,344
0201BA	Compaq ProLiant 5000 Pentium Pro 200/512 CPU (For adding CPUs 2, 3, 4 to the ProLiant 5000)	1,063
0201CA	Compaq ProLiant 6000 6/200-512 Advanced Server, 128MB, 4.3GB SuperServer system	10,635
0201CB	Same as 0201CA with Smart 2/DH array controller and two 4.3GB hot swap UW hard drives	13,667
0210AB	Compaq 2.1GB Hot-pluggable Wide-Ultra SCSI 2 1" drive	805
0250BA	32MB Memory Expansion (2x16MB SIMM 32 Bit/70ns) for Laser printers $196	
0250DA	16MB Memory Expansion (1x16MB SIMM 32 Bit/70ns) for Laser printers	98

The following CLINs have been deleted from the contract:

CLIN	DESCRIPTION
0007DA	Cabletron - High-Speed Local Ethernet Bridge Module
0110BA	850MB Hard Disk Drive
0150AA-JE	Microwave LAN Equipment
1020AA-AD	SafetyNet VirusNet LAN
2310AA-BA	FTP TCP/IP software

Electronic Data Systems (EDS)
EDS Web Site http://www.eds-ms.com/pclan
EDS: 1-800-241-2143

NCTAMS LANT Points of Contact
Technical Specifications and Support Branch
Ordering: Shirley Dunbar
Phone: (757) 445-1493; DSN 565
E-mail : shirley_dunbar@ccmail.nctamslant.navy.mil
Tech Support: John Mclaurin (757) 445-2568; DSN 565
E-mail : john_mclaurin@ccmail.nctamslant.navy.mil

SEWP II

The Scientific and Engineering Workstation Procurement II (SEWP II) was conducted using the Full and Open Competition Procedures as defined in Federal Acquisition Regulation (FAR) Subpart 6.1. This vehicle is an indefinite delivery, indefinite quantity procurement consisting of seventeen contracts that offer a wide range of advanced technology UNIX workstations, peripherals, network equipment, and network services to NASA, NASA contractors, Federal Agencies and their contractors, Navy, Army, and Air Force.

What's in the SEWP II?

SEWP II contains several vendors that supply a variety of UNIX and NT workstations as well services such as software, maintenance, integration, installation, assistive technology and advanced studies.

- **Contract 1 (NAS5-96006) Electronic CAD Workstation.**

▶

These workstations will be used for the development of custom and semi-custom Very Large Scale Integration(VLSI) chip designs for the designing, routing and placing of printed circuit board layouts. Specific functions include schematic capture, timing tests, simulations, route and place and test and verification of physical components.
Selected Vendor: Sun Microsystems

- **Contract 2 (NAS5-96002) Mechanical CAD Workstation.** These workstations will be used to support mechanical, structural, and thermal engineering tasks including structural analysis, mechanical design and thermal analysis.
Selected Vendor: Hewlett-Packard

- **Contract 4 (NAS5-96004) Network Data Server.** These workstations will be used to house large data volumes and large databases. Applications are typically based on commercial DBMS packages.
Selected Vendor: IBM

- **Contract 5 (NAS5-96005) 3D Graphics Workstation.** These workstations will be used to provide the highest quality in the visual representation of data to the user.
Selected Vendor: Silicon Graphics, Inc.

- **Contract 6 (NAS5-96006) Software Development Workstation.** These workstations will be used to support software engineering, full life cycle software development and maintenance, proof of concept and prototype development, client application development and other XPG4 UNIX based development efforts.
Selected Vendor: Sun Microsystems, Inc.

- **Contract 7 (NAS5-96151, NAS5-96007, NAS5-96010)** General Purpose Workstation. These workstations will be used for the deployment of internally developed, highly available XPG4 UNIX based applications. These are native X Windows client applications running on the local workstation and accessing server resources on NASA LANs and WANs.
Selected Vendors: Compaq, Digital, UNISYS

- **Contract 8 (NAS5-96002) GIS Workstation.** These workstations will be used to support geographic analysis, data integration, and image processing. These systems will provide support for Geographic Information Systems (GIS) analysts, earth and environmental scientists, and the public.
Selected Vendor: Hewlett-Packard

- **Contract 9 (NAS5-96009) Supporting Equipment.** This class consists of input and output peripherals and other equipment which support and complement the full implementation of XPG4 UNIX based workstations throughout NASA.
Selected Vendor: Government Technology Sales, Inc.

- **Contract 10 (NAS5-96010) Network Equipment.** This class consists of a range of network equipment in support of the full implementation of XPG4 UNIX based workstations in the NASA network environment.
Selected Vendor: Unisys

- **Contract 11 (NAS5-96009) Administrative File Server**. This class provides a server operating system (OS), complementary client operating systems and associated software which is capable of handling administrative file server and client functionality on a variety of hardware platforms within the administrative Government computing environment.
Selected Vendor: Government Technology Sales, Inc.

- **Contract 12 (NAS5-96012) Storage Devices .** This class consists of storage devices; e.g. hard disks and tape systems which can be used by workstations in all of the classes listed above.
Selected Vendor: Sylvest Management Systems, Inc.

- **Contract 13 (NAS5-96005) Compute Server.** The Computer Server class of systems and services will be used to provide systems able to perform very computer-intensive traditional optimized applications such as modeling, and mathematical analysis.
Selected Vendor: Cray

- **Contract 14 (NAS5-97047) 3rd Party Software**
Selected Vendor: ECS

- **Contract 15 (NAS5-97048) 3rd Party Maintenance/ Integration/Installation**
Selected Vendor: Dynatech Integrated Systems Corp

- **Contract 16 (NAS5-97049, NAS5-97050)**
System Development
Selected Vendors: Zero & One , Astrox

- **Contract 17 (NAS5-97051) Assistive Technology**
Selected Vendor: NCSS

- **Contract 18 (NAS5-32898) 3rd Party Peripherals**
Selected Vendor: GMR

Announcements: Doug Hanson is no longer head of SEWP operations. He has been transferred to another project management position at NASA's Goddard Space Flight Center (GSFC). Doug had been with the SEWP contracting project for six years. His previous SEWP responsibilities have been taken over by Joe Barksdale. He can be reached at (301) 286-8652 or jbarksda@pop200.gsfc.nasa.gov.

For all SEWP inquiries, continue to call NCTAMS LANT for up-to-date information.

All Navy SEWP orders must be submitted to NCTAMS LANT. Please mail your signed SEWPII Delivery Order with the surcharge included on the order using the vendor's Surcharge CLIN, the associated vendor configuration approval, and a 2275 or 2276A for the Navy 1 percent surcharge to the Navy Ordering Representative as stated below.

All Navy orders should be sent to:
Technical Specifications and Support Branch
Code N811.2
NCTAMS LANT
9625 Moffett Ave
Norfolk, VA 23511-2784

NCTAMS LANT Points of Contact
Technical Specifications and Support Branch

Ordering:	SherleyAnn Parks
E-mail:	sherleyann_parks@ccmail.nctamslant.navy.mil
Phone:	(757) 445-1493; DSN 565-1493
Tech Support:	Rick Paquin
E-Mail:	rick_paquin@ccmail.nctamslant.navy.mil
Phone:	(757) 445-2568; DSN 565-2568

ULANA II Is Now Year 2000 Compliant

Both ULANA II contractors, EDS and TRW, have their hardware and software products clearly identified as Y2K. Be sure to check the latest Approved Products List (APL) on our web site, www.chips.navy.mil or link to the contractors' sites, www.ulana2.com for TRW and www.eds-ms.com for EDS.

Each contractor’s web site offers a search engine to locate the desired products. The APLs are typically updated monthly with the latest change for EDS dated 23 Jan 98 and TRW’s dated 13 Jan 98.

The Y2K certification has been completed by either the OEM or the contractor and certified by the Air Force.

SBIS - Army IDIQ

The latest modification, number 103 dated Jan 98, incorporates new CLINs, price reductions and deletions.

CLIN	DESCRIPTION	PRICE
IBM Deletions		
5111AA	RS/6000 7025 MODEL F30 SERVER, 1 TO 2 USER LICENSE	$8,966.00
5111AD	233 MHZ POWERPC 604E PROCESSOR FOR 7025-F30	1,455.00
5112AA	5GB/10GB 8MM INTERNAL TAPE DRIVE	3,690.56
5112AC	2/2GB SCSI-3 FAST/WIDE HOT-SWAP DISK DRIVE	1,397.00
5112AF	PCI ETHERNET AUI/RJ-45 ADAPTER	145.00
5112AL	ASYNCH TERMINAL/PRINTER CABLE EIA-232	33.00
5112AN	64MB HD3 MEMORY CARD	1,196.00
5112AS	RJ-45 TO DB25 CONVERTER CABLE	88.00
5112AT	128 PORT ASYNCH 4.5 CONTROLLER CABLE 4/5 METER (15FT)	44.00
5112AU	REMOTE ASYNCH NODE 16 PORT EIA-232	1,105.99
5112AV	128 PORT ASYNCH CONTROLLER ISA BUS	883.99
5112AY	PCI SCSI-2 SE FAST/WIDE ADAPTER	266.00
5112BB	8 PORT ASYNCH ADAPTER EIA-2323	615.00
5112BE	4-PORT MULTIPROTOCOL COMM CONTROLLER, ISA BUS	1,221.00
5112BF	4-PORT MULTIPROTOCOL IF CABLE	
5112BG	MULTIPROTOCOL MODEM ATTACHMENT CABLE-EIA-232/V.24	67.32
5112BL	SCSI 6-PACK #3 (CONTROLLER, CABLES, ETC)	449.00
5112BM	128MB DIMM MEMORY	2,560.00
5112BN	SCSI 6-PACK #2 (CONTROLLER, CABLES, ETC)	481.00
5112BQ	4.5GB ULTRASCSI HOT SWAP DRIVE	1,998.00
5112BS	PCI SCSI-2 DIFERENTIAL FAST/WIDE ADAPTER	444.00
5112BW	32MB DIMM MEMORY	598.00
Cabletron Deletions		
5145BQ	9-PORT ETHERNET MULTICHANNEL ASSIGNMENT MODULE (RJ45S)	1,858.00
5145BT	24-PORT ETHERNET MULTICHANNEL ASSIGNMENT MODULE (50-PIN	3,140.00
5147AK	FIBER INTERFACE MIM (CABLETRON)	3,105.29
5147AL	TWISTED PAIR MIM (CABLETRON)	542.77
5147NH	4 PORT FDDI CONCENTRATOR MODULE (MM)	4,452.03
5147VV	24 PORT 10BASET ETHERNET SWITCH WITH EMPTY UPLINK	4,535.00
5147VW	12 PORT 10BASET ETHERNET WITH EMPTY UPLINK	3,440.00
5147VX	DUAL 100BASETX UPLINK EXPANSION CARD 10BASET SWITCH NOT	1,413.00
5147VY	DUAL 100BASEFX UPLINK EXPANSIOIN CARD 10BASET SWITCH	1,484.00
5205AQ	VLAN MANAGER SERVER FOR SGI IRIX (CD ROM)	3,707.72
5205AR	VLAN MANAGER SERVER FOR IBM AIX (CD ROM)	3,707.72
5205AS	VLAN MANAGER SERVER FOR HP/UX (CD ROM)	3,707.72
5205AU	VLAN MANAGER CLIENT FOR SGI IRIX (CD ROM)	736.82
5205AV	VLAN MANAGER CLIENT FOR IBM AIX (CD ROM)	736.82
5205AW	VLAN MANAGER CLIENT FOR HP/UX (CD ROM)	736.82
5205AY	SPEL 1.0 FOR WINDOWS CD	1,796.99
5205AZ	SPEL 1.0 FOR WINDOWS DISK	64.76
Global InSync Deletions		
5113PN	8X SPEED CD-ROM READER	72.00
IBM Price Reductions		
5290HD	AIX VE-V4.2 UPGRADE ADVANCED SERVER 1-2 USER	245.82
5290HE	AIX V3-V4.2 UPGRADE DESIGNATED SYSTEM USER (1 USER)	24.05
5290HJ	AIX V4.1-V.2 UPGRADE ADVANCED SERVER 1-2 USER	245.82
Jetforms Addition		
5202AC	FORMFLOW SOFTWARE DEVELOPMENT/STARTER KIT	777.43
Cabletron Addition		
5147WW	SMARTSWITCH ETHERNET INB MODULE W/FIBER CONNECTIONS (36)	18,994.30
IBM Additions		
5190UT	ETHERNET 10/100MBPS MC ADAPT. FOR 39H	592.75
5190UV	ETHERNET 10/100MBPS MC ADAPT. FOR 595	592.75
5190UW	ETHERNET 10/100MBPS MC ADAPT. FOR R24	592.75

The SBIS contract does not identify the Y2K compliant products. ▶

Please visit the Navy's web site or the contractor's site at www.sbis.idiq.com/sbisidiq or call toll free 1-800-882-4347 for a free copy of their catalog and more information.

NTOPS Cordant (a Tracor Company)

N68939-96-D-0007

For the most up-to-date status on products and prices please visit Cordant's Web site at cad2www.cordant.com/ntops/ntops.htm or NCTAMS LANT's web site. Cordant's NTOPS Customer Support Group may be reached at 1-888-798-6867 for CONUS and 1-703-758-7080 for OCONUS. Cordant's dedicated NTOPS' BBS can be reached at 1-800-382-7058.

The Cordant IDIQ contract is open to the Navy and Marine Corps activities, DoD agencies (including the Air Force and Army) and civilian agencies. The following CLIN list incorporates all fifty-four mods for the NTOPS-Cordant Contract.

Microsoft Windows 95 is now the default operating system being delivered with every system (except 0002AM/AQ/AV/AX/AY, these systems are delivered with Microsoft Windows NT Workstation.) Microsoft Windows For Workgroups 3.11 can be substituted for Windows 95 at the time the system is ordered by ordering the 'No Cost' CLIN 0052FD (for floppy disk media). Windows NT Workstation can be ordered as an upgrade CLIN 0050CD (for CD-ROM media) from Windows 95 for $119.34 and is also a factory install that must be ordered at the same time the system is ordered.

When ordering from NTOPS, don't forget the customized delivery order CLIN (0060AA). The purpose of CLIN 0060AA is to offer the ability for customers to order a complete solution or group of products that may include products that are not currently on the contract, all of which can be ordered on a single delivery order.

Additionally, Cordant may offer bottom-line discounts based upon the type and quantity of products being ordered. Products not currently available on the contract referred to as other direct costs (ODCs) can be included in the assigned solution CLIN, 0060AA, but the total value of the ODCs must be less than 20 percent of the value of the delivery order. The limit may be exceeded with NAVICP's approval. Customers should contact Cordant and request a combined quote for the products that they need. Cordant will offer a firm fixed price quote (including the contract usage fee), utilizing the items available from the NTOPS contract B-tables and pricing for the ODCs.

* Desktop Monitors are separately orderable as CLIN 0014xx and Desktop Hard Disk Drives (HDD) are separately orderable as CLIN 0009xx (except when CLIN 0002AQ is ordered.)

CLIN	DESCRIPTION	PRICE
0002AM	EVEREX STEP SP/Pro Intel 200Mhz Pentium Pro w/ 0MB HDD 32MB EDO RAM expandable to 512MB, 256KB CPU cache, 3.5" FDD, Logitech 2-button serial mouse, 104-key enhanced keyboard, MS Windows 95, Matrox Millenium II w/ 4MB WRAM video card	$1,668.72
0002AQ	EVEREX IT-21 WORKSTATION Intel 266Mhz Pentium II processor w/256k cache, 64MB EDO RAM expandable to 512MB, PS/2 104-key keyboard & 2-button mouse, Action Tec PCMCIA rear load PC card reader, ATX mid tower w/ 235W power supply, 7 drive bays total-(3) external 5.25", (2) external 3.5", (2) internal 3.5", Western Digital AC33100 3.1GB HDD, 3.5" FDD, Matrox Millenium II w/ 4MB WRAM video card, Creative Labs Sound Blaster 64 AWE sound card, 14W speakers, Intel Pro 100 10/100 ethernet card, NEC 16x IDE CD-ROM Drive, Goldstar 17" color monitor, MS Windows NT 4.0 Workstation.	2,694.84
0002AR	EVEREX TEMPO K AMD K6 MMX 200 Mhz w/ 0 HDD, MS Windows 95, 16MB EDO RAM expandable to 512MB, 3.5" FDD, 512k synchronous pipeline burst Level2 cache, Matrox Mystique PCI video accelerator card w/ 2MB SGRAM, 104-key enhanced keyboard, Logitech 2-button PS/2 mouse	915.96
0002AS	EVEREX TEMPO K AMD K6 MMX 233 Mhz w/ 0 HDD Same as CLIN 0002AR but with an AMD K6 MMX 233Mhz processor	1,002.66
0002AT	STEP SP PLUS Intel MMX 166 Mhz w/ 0 HDD, 16MB EDO RAM expandable to 512MB, 3.5" FDD, MS Windows 95, 512k synchronous pipeline burst Level2 cache, Matrox Mystique PCI video accelerator card w/ 2MB SGRAM, 104-enhanced keyboard, Logitech 2-button mouse	848.64
0002AU	STEP SP PLUS Intel MMX 200 w/ 0 HDD Same as CLIN 0002AT but with an Intel MMX 200Mhz processor	874.14
0002AV	STEP DP/PRO DUAL Intel 200 Mhz PENTIUM PRO w/ 0 HDD w/256k cache, 32MB EDO RAM expandable to 512MB, 3.5" FDD, MS Windows NT Workstation, 104-key enhanced keyboard, Logitech 2-button mouse, Matrox Millenium II w/ 4MB WRAM video card	2,416.38
0002AX	EVEREX STEPstation 2 Intel PENTIUM II 266 Mhz WORKSTATION MS Windows NT Workstation 32MB EDO RAM expandable to 788MB, 3.5" FDD, 512k single edge contact cache, Matrox Millenium II w/ 4MB WRAM video card, 104-key enhanced keyboard, PS/2 2-button mouse	1,501.44
0002AY	EVEREX STEPstation 2 PENTIUM II 233 WORKSTATION. Same as SLIN 0002AX but with an Intel Pentium II 233Mhz processor	1,402.50
0003AC	TRACKBALL UPGRADE CH Products, Trackball PRO, 400-501	73.44

CLIN	DESCRIPTION	PRICE
	Serial Trackball, V. 1.0, 2.25" Diameter Ball	
0003AF	MATROX MYSTIQUE VIDEO ADAPTER w/ 4MB RAM UPGRADE Factory Installed only for SLINS 0002AF/AG/AH/AJ/AK/AL/AM/AN/AP	35.70
0005AS	EVEREX STEPNOTE 150 MMX NOTEBOOK same as 0005AQ w/ 2.1GB HDD	2,754.00
0005AT	EVEREX STEPNOTE 150 MMX NOTEBOOK same as 0005AQ w/ 2.1GB HDD & 20x CD-ROM Drive	2,907.00
0005AU	PALM PILOT PERSONAL EDITION P/N 80200U	224.40
0005AV	PALM PILOT PROFESSIONAL EDITION P/N 80201U	331.50
0005AW	EVEREX STEPNOTE 5 166 MMX NOTEBOOK w/ 2.1GB HDD Intel Pentium MMX 166Mhz, 12.1" TFT SVGA(800x600) Active Matrix Display, 256k synchronous cache, 16MB EDO RAM upgradeable to 48MB, Chips and Technologies PCI video accelerator w/ 2MB DRAM, zoom video support, modular 2.1GB HDD, modular 3.5" FDD, 2 PCMCIA slots, 16-bit audio, speakers and microphone, 2 media bays, Lithium ion battery, carrying case, MS Windows 95	2,584.68
0005AX	EVEREX STEPNOTE 5 166 MMX NOTEBOOK w/2.1GB HDD same as 0005AW with a 10x CD-ROM Drive	2,718.30
0005AY	EVEREX STEPNOTE SC 150 NOTEBOOK w/ 1.4GB HDD, 10x CD-ROM Drive, Intel Pentium 150Mhz, 12.1 TFT SVGA (800X600) Active Matrix Display, 256k synchronous cache, 16MB EDO RAM upgradeable to 80MB, a NeoMagic 128 bit video accelerator w/ 1.5MB RAMBUS video DRAM, zoom video support, 3.5" FDD, 2 PCMCIA slots, 16-bit audio, speakers, microphone, 33.6kbps fax/modem, glide pointing device, carrying case, NiMH battery, MS Windows 95	2,580.60
0005AZ	EVEREX STEPNOTE SC 150 NOTEBOOK w/ 2.1GB HDD, 10x CD-ROM Drive; Same as 0005AY with a 2.1GB HDD	2,631.60
0005BA	EVEREX STEPNOTE SC 150 MMX NOTEBOOK w/ 1.4GB HDD, 10x CD-ROM Drive; Same as 0005AY with MMX Pentium	2,648.94
0005BB	EVEREX STEPNOTE SC 150 MMX NOTEBOOK w/ 2.1GB HDD, 10x CD-ROM Drive, Same as 0005AY with MMX Pentium	2,694.84
0005BC	EVEREX STEPNOTE SC 166 MMX NOTEBOOK w/ 1.4GB HDD, 10x CD-ROM, Same as 0005AY with 166Mhz MMX Pentium	2,776.44
0005BD	EVEREX STEPNOTE SC 166 MMX NOTEBOOK w/ 2.1GB HDD, 10x CD-ROM, Same as 0005AY with 166Mhz MMX Pentium	2,833.56
0006AC	TRIMM 1-BAY EXPANSION CABINET for use with CLINS 0005AL through 0005AT	127.50
0006AD	PALM PILOT MODEM P/N 10201U	118.32
0006AE	PALM PILOT MODEM AC ADAPTER P/N 10202U	15.30
0006AF	PALM PILOT NETWORK HOTSYNC (1 PACK) P/N 90106U	61.20
0006AG	PALM PILOT CRADLE FOR WINDOWS P/N 10109U	22.44
0006AH	HOT SYNC CRADLE FOR LAPTOP P/N 10104U	15.30
0006AJ	PALM PILOT MODEM CABLE P/N 1011U	13.26
0006AK	STYLUS (3 PACK) P/N 10108U	4.08
0006AL	SLIM LEATHER CARRYING CASE	18.36
0006AM	LEATHER BELT CLIP CASE	18.36
0006AN	DELUXE LEATHER CASE	48.96
0006AP	EVEREX STEPNOTE 5 PORT REPLICATOR 15-pin external monitor port, 16C550A compatible serial port, 15-pin game and MIDI port, SPP/EPP/ECP parallel port, PS/2 keyboard port, PS/2 mouse port. Only for use with Everex StepNote 5 Notebooks.	93.84
0006AQ	EVEREX STEPNOTE 5 PORT REPLICATOR BUNDLE Same as SLIN 0006AP with one AC adapter, one PS/2 keyboard and one PS/2 mouse included. Only for use with Everex StepNote 5 Notebooks.	163.20
0006AR	EVEREX STEPNOTE 5 DOCKING STATION P/N KIT-00661-4500 Two PCI bus slots, 15-pin VGA monitor port, 9-pin serial port, 25-pin serial port with 16550 UART and FIFO support, 25-pin parallel port supporting both ECP and EPP standards, AT keyboard port, PS/2 mouse port, stereo line-in/line-out, microphone-in, one 5.25" or 3.5" external access bay, one 3.5" internal bay, power switch, locking switch, reset switch and an integrated power supply.	459.00
0006AS	EVEREX STEPNOTE 5 DOCKING STATION - BUNDLE same as SLIN 0006AR w/a AT keyboard and PS/2 mouse.	490.62
0007AA	8MB RAM FOR DESKTOPS, Everex, Kit-00343-0000, Two 70ns 4MB SIMMS	40.80
0007AB	16MB RAM FOR DESKTOPS, Everex, Kit-00362-0000, Two 70ns 8MB SIMMS	64.26
0007AC	32MB RAM FOR DESKTOPS, Everex, Kit-00345-0000, Two 70ns 16MB SIMMS	116.28
0008AF	StepNote 5 16MB MEMORY KIT - for use with CLINS 0005AL through 0005AT	106.08
0008AG	StepNote 5 32MB MEMORY KIT - for use with CLINS 0005AL through 0005AT	212.16
0008AH	PILOT 1MB MEMORY UPGRADE	96.90

▶

CLIN	DESCRIPTION	PRICE
	P/N 10200U	
0008AJ	STEPNOTE SC 16MB EDO MEMORY UPG P/N KIT-00486-0000X	112.20
0008AK	STEPNOTE SC 32MB EDO MEMORY UPG P/N KIT-00487-0000X	229.50
0008AL	STEPNOTE SC 64MB EDO MEMORY UPG P/N KIT-00488-0000X	530.40
0009AC	WESTERN DIGITAL, AC22000, 2GB EIDE HDD	150.96
0009AD	WESTERN DIGITAL, AC33100, 3.1GB EIDE HDD	202.98
0009AE	SEAGATE 1GB ULTRA SCSI HDD, ST31055N	317.22
0009AF	SEAGATE 2.1GB ULTRA SCSI HDD, 5400 RPM spindle, ST32155N	452.88
0009AG	SEAGATE 2.1GB ULTRA SCSI HDD, 7200 RPM reliability, ST32272N	601.80
0009AH	SEAGATE 4.3GB ULTRA SCSI HDD, ST34371N	768.06
0009AJ	WESTERN DIGITAL 4GB EIDE HDD, AC34000	237.66
0009AK	SEAGATE BARRACUDA 4LP 7200RPM 4.3GB Ult Wde SCSI HDD, ST34371W	782.34
0009AL	SEAGATE BARRACUDA 4LP 7200RPM 9.1GB Ultra SCSI HDD, ST19171N	1,114.86
0009AM	SEAGATE BARRACUDA 4LP 7200RPM 9.1GB Ult Wde SCSI HDD, ST19171W	1,164.84
0009AN	SEAGATE CHEETA 4LP 10,000RPM 4.5GB Ultra SCSI HDD, ST34501N	846.60
0009AP	SEAGATE CHEETA 4LP 10,000RPM 4.5GB Ult Wde SCSI HDD, ST34501W	896.58
0009AQ	SEAGATE CHEETA 4LP 10,000RPM 9.1GB Ultra SCSI HDD, ST19101N	1,377.00
0009AR	SEAGATE CHEETA 4LP 10,000RPM 9.1GB Ult Wde SCSI HDD, ST19101W	1,434.12
0009AS	SEAGATE ELITE 23 5400RPM 23.2GB Ultra SCSI HDD, ST423451N	2,438.82
0009AT	SEAGATE ELITE 23 5400RPM 23.2GB Ult Wde SCSI HDD, ST423451W	2,495.94
0009AU	IOMEGA JAZ DRIVE W/ 1GB MEDIA (EXTERNAL), 10134	402.90
0009AV	IOMEGA JAZ DRIVE W/ 1GB MEDIA (INTERNAL), 10133	301.92
0009AW	IOMEGA ZIP SCSI DRIVE (EXTERNAL), 10011	147.90
0009AX	IOMEGA ZIP PARALLEL DRIVE (EXTERNAL), 10012	147.90
0009AY	IOMEGA ZIP SCSI DRIVE (INTERNAL), 10341	147.90
0009AZ	IOMEGA JAZ MEDIA SINGLE PACK, 10150	106.08
0009BA	IOMEGA JAZ MEDIA THREE PACK,10387	257.04
0009BB	IOMEGA ZIP MEDIA SINGLE PACK, 10020	14.28
0009BC	IOMEGA ZIP MEDIA SIX PACK, 10297	74.46
0010AB	STEPNOTE 5 1.4GB HDD, TOSHIBA, PER-01194-0000	229.50
0010AC	STEPNOTE 5 2.1GB HDD, TOSHIBA	272.34

CLIN	DESCRIPTION	PRICE
	or HITACHI	
0011AA	INTERNAL 24x CD-ROM DRIVE, GOLDSTAR, P/N CDR-824BB	69.36
0011AC	12x SCSI CD-ROM DRIVE, PLEXOR PX-12TSI-BP	272.34
0011AE	INTERNAL 16x CD-ROM CHANGER, NAKAMICHI, P/N MJ5.16 Capacity of 5, SCSI-2	255.00
0011AF	INTERNAL 12x CD-ROM CHANGER, PANASONIC, SQ-TC512N EIDE interface with ATAPI support	268.26
0011AG	INTERNAL 4x/6x CD-ROM, YAMAHA W/EZ-PRO SW	636.48
0011AH	RECORDABLE CD - 74 MINUTES	4.08
0012AA	EXTERNAL 4x/600MB CD-ROM DRIVE, SYNCHROME TECHNOLOGY, Maestro 01-05010-01, Parallel	150.96
0013AC	270MB REMOVABLE MAGNETIC MEDIA HDD, PowerUser, P/N DR4547	318.24
0013AD	SYQUEST 270MB CARTRIDGE (media for 0013AC), SQ327	51.00
0013AE	500MB IDE REMOVABLE HDD, REM-STOR, REM-545-ADP	229.50
0014AA	14" DIAGONAL 1024x768, SVGA, .28mm DP, MAGNAVOX, CM2099 OR WEN OR GOLDSTAR, 1465DLSDP	179.52
0014AB	17" DIAGONAL 1280X1024, .28mm DP, Desktop Displays, DDU-1728 OR WEN, US 176, OR GOLDSTAR, GS-1725S,	362.10
0014AC	15" DIAGONAL 1280x1024, .28mm DP, WEN OR GOLDSTAR	212.16
0014AD	WEN STN 10.4" LCD MONITOR, 0.239x0.239 DP, 800x600, VESA DPMS/EPA compatible	652.80
0014AE	WEN TFT 12.1" COLOR LCD MONITOR, 0.3075x0.3075 DP, 800x600, active matrix, VESA DPMS/EPA compatible	2,310.30
0014AF	WEN STN 12.1" LCD MONITOR, 0.3075x0.3075 DP, 800x600, VESA DPMS/EPA compatible	1,944.12
0014AG	WEN TFT 13.8" LCD MONITOR, 0.273x0.273 DP, 1024x768, VESA DPMS/EPA compatible	2,990.64
0014AH	WEN 20" FLAT SQUARE TUBE COLOR MONITOR, .28mm DP, 1600x1200, VESA/EPA compatible	945.54
0014AJ	WEN 21" FLAT SQUARE TUBE COLOR MONITOR, .28mm DP, 1600x1200, VESA/EPA compatible OR GOLDSTAR 21", GS-21I	1,244.40
0015AA	400MB INTERNAL TAPE BACKUP DRIVE, IOMEGA DITTO EASY 800 TRAVAN IDE, w/ Two Cartridges/Software OR HP/COLORADO T1000 400MB	87.72
0015AB	1GB INTERNAL TAPE BACKUP DRIVE, TANDBERG DATA, TDC-4120 SCSI, 5.25",	667.08

CLIN	DESCRIPTION	PRICE
	w/ Two Cartridges/SCSI Controller/Software	
0015AC	400MB INTERNAL SCSI TAPE BACKUP DRIVE, SEAGATE SGT-T800R-FMPBE	98.94
0015AD	13GB INTERNAL SCSI-2 TAPE BACKUP DRIVE, TANDBERG, 6701 13GB native/26GB using ALDC data compression 180MB/min, 5.25"	2,155.26
0015AE	13GB EXTERNAL SCSI-2 TAPE BACKUP DRIVE, TANDBERG, 6751 13GB native/26GB using ALDC data compression 180MB/min, 5.25"	2,348.04
0015AF	13GB IMATION MLR TAPE CARTRIDGE, 430632, FOR CLINS 0015AD/AE	55.08
0015AG	DRY PROCESS CLEANING CARTRIDGE FOR CLINS 0015AD/AE	27.54
0015AH	8GB SEAGATE SCORPION DAT DRIVE W/ SEAGATE CLEANING KIT AND DAT TAPES (5 PACK) P/N STD-28000N W/SGT-91301 & SGT-32000	824.16
0016AA	PANASONIC KX-P3123, MONOCHROME 24-PIN DOT-MATRIX PRINTER 80 Column, 240CPS, Push/Pull Tractor	229.50
0016AB	CANON BJ-30, MONOCHROME BUBBLEJET NOTEBOOK PRINTER 277 CPS, NLQ, w/ Battery/Recharger/ AC Adapter/Cable	346.80
0016AC	HP DESKJET 692C, C4582A 600 dpi, 512k RAM, HP Res. Enhancement Technology(REt), 1-5 PPM black, 1-3 PPM color	292.74
0016AD	BROTHER HL-1660, 17PPM LASER PRINTER 1200x600 dpi(Graphics), 600x600 dpi(Text), 4MB RAM(up to 66MB), PS level 2, PCL 5e	1,252.56
0016AE	1MB MEMORY UPGRADE for BROTHER HL-1260/1660, 0016AD	44.88
0016AF	2MB MEMORY UPGRADE for BROTHER HL-1260/1660, 0016AD	89.76
0016AG	4MB MEMORY UPGRADE for BROTHER HL-1260/1660, 0016AD	169.32
0016AH	COLOR KIT FOR DOT-MATRIX, PANASONIC, KX-PCK11 FOR 0016AA	40.80
0016AK	HP LASERJET 6Lxi, C3996A, 6PPM LASER PRINTER, 600x600 dpi, HP RET	378.42
0016AL	1MB MEMORY UPGRADE for HP LASERJET 6Lxi, 0016AK	48.96
0016AM	2MB MEMORY UPGRADE for HP LASERJET 6Lxi, 0016AK	76.50
0016AN	4MB MEMORY UPGRADE for HP LASERJET 6Lxi, 0016AK	103.02
0016AS	HP LASERJET 5Si, 24PPM, 40Mhz AMD 29040 RISC, 4MB RAM (up to 132MB), HP PCL 6	2,429.64
0016AT	HP LASERJET 5SiMX, 24PPM, 40Mhz AMD 29040 RISC, 12MB RAM(up to 76MB), HP PCL 5 &	3,533.28

CLIN	DESCRIPTION	PRICE
	Adobe PS level 2	
0016AW	HP LASERJET 6Pxi, C4213A, 600 dpi, HP RET, 8PPM	724.20
0016AX	HP LASERJET 6MP, 8PPM, 24Mhz Intel 80960 JF RISC, 2MB RAM(up to 35MB), HP PCL 6 & Adobe PS level 2	868.02
0016AY	HP COLOR LASERJET 5, 10PPM B&W/ 3PPM COLOR, 24Mhz AMD 29040 RISC, 20MB RAM (up to 84MB), HP PCL 5	4,182.00
0016AZ	HP DESKJET 1600C, 8PPM B&W/2PPM COLOR, Intel 32mhz RISC i80960KB, 4MB RAM(up to 100MB), HP PCL 5	1,284.18
0016BA	HP 6100 SCANNER	737.46
0016BB	HP JETDIRECT ADAPTER CARD (For use w/ 0016AP/AR/AQ/AS/AT/AY/AZ)	281.52
0016BC	4MB SIMM for LASERJET (For use w/ 0016AP/AQ/AR/AS/AT/AW/AX/AY/AZ)	23.46
0016BD	8MB SIMM for LASERJET (For use w/ 0016AP/AQ/AR/AS/AT/AW/AX/AY/AZ)	42.84
0016BE	16MB SIMM for LASERJET (For use w/ 0016AP/AQ/AR/AS/AT/AW/AX/AY/AZ)	99.96
0016BF	HP JETDIRECT EX PLUS (External) PRINT SERVER (For use w/ 0016AW/AX)	262.14
0016BG	ADOBE POSTSCRIPT SIMM, LASERJET 5si (For use w/ 0016AS)	363.12
0016BH	HP JET DIRECT CARD ETHERNET, 2550B	278.46
0016BJ	HP JET DIRECT CARD TOKEN RING, 2555B	467.16
0016BK	HP JET DIRECT CARD ETHERNET/BNC/RJ-45, 2552B	323.34
0016BL	HP 5si DUPLEX OPTION, C3762A, (For use w/ 0016AS/AT)	418.20
0016BM	HP DESKJET 1600CM, C3541A	1,872.72
0016BN	ADOBE POSTSCRIPT UPG KIT FOR DESKJET 1600C (CLIN 0016AZ), PC3542A	449.82
0016BP	ADOBE POSTSCRIPT UPG KIT FOR HP COLORJET 5 (CLIN 0016AY), C3963A	482.46
0016BQ	HP DESIGNJET 750C PLUS PLOTTER (D/A1 SIZE), C4708A Print resolution of 600dpi in monochrome(for CAD drawings and HP media only), addressable resolution of 600dpi in HPGL/2 color, 11MB RAM (up to 75MB), HP-GL(7568B), HP-GL/2, RTL, PJL	4,655.28
0016BR	HP DESIGNJET 750C PLUS PLOTTER (E/A0 SIZE), C4709A Print resolution of 600dpi in monochrome(for CAD drawings and HP media only), addressable resolution of 600dpi in HPGL/2 color, 11MB of RAM (up to 75MB), HP-GL(7568B), HP-GL/2, RTL, PJL	5,431.50
0016BS	LEXMARK OPTRA S1250, 43J1000 12PPM(8PPM at 1200 dpi), 33Mhz Intel i960JF processor, 4MB RAM, true 1200dpi, 600dpi with PQET	1,032.24

►

CLIN	DESCRIPTION	PRICE
	(Print Quality Enhancement Technology), 300dpi with PQET, PS 2, Enhanced PCL6	
0016BT	LEXMARK OPTRA S1250N, 43J1038 Same as CLIN 0016BS and includes an Ethernet 100BaseTX & 10BaseT card using EtherExpress Pro/100 technology with auto-speed negotiation.	1,323.96
0016BU	LEXMARK MARKNET 10/100TX NETWORK INTERFACE CARD, 44H0003	281.52
0016BV	HP LASERJET 4000, C4118A 17PPM, 100Mhz RISC processor, 4MB RAM, HP PCL 6, HP PCL 5e & PS LVL2 Emulation, 600 sheet standard, 1-100 sheet tray & 1-500 sheet tray	1,071.00
0016BW	HP LASERJET 4000T, C4119A 17PPM, 100Mhz RISC processor, 4MB RAM, HP PCL 6, HP PCL 5e & PS LVL2 Emulation, 600 sheet standard, 1-100 sheet tray & 2-250 sheet trays	1,214.82
0016BX	HP LASERJET 4000N, C4120A 17PPM, 100Mhz RISC processor, 8MB RAM, HP PCL 6, HP PCL 5e & PS LVL2 Emulation, 600 sheet standard, 1-100 sheet tray & 1-500 sheet tray. HP JetDirect 600N Print Server	1,382.10
0016BY	HP LASERJET 4000TN, C4121A 17PPM, 100Mhz RISC processor, 8MB RAM, HP PCL 6, HP PCL 5e & PS LVL2 Emulation, 600 sheet standard, 1-100 sheet tray & 2-250 sheet trays, HP JetDirect 600N Print Server	1,523.88
0016BZ	LEXMARK OPTRA SC 1275 COLOR PRINTER 12PPM Black/3PPM Color, 66Mhz RISC Intel i960 processor, 16MB RAM, 600 dpi	3,740.34
0016CA	LEXMARK OPTRA SC 1275N COLOR LASER PRINTER true four-color process, 12PPM Black/3PPM Color, 66Mhz RISC Intel i960 processor, 32MB RAM, 600dpi, 1200 image quality, PCL 5 w/color emulation, PCL 6 mono emulation, PS Level 2 emulation, Ethernet 100BaseTX/10BaseT	4,152.42
0016CB	HP JET DIRECT 600N INTERNAL PRINT SERVER for ethernet 10/100Base TX Networks, J3113A	316.20
0017AA	INTERNAL SEND/RCV FAX MODEM (DESKTOPS) Cardinal, 33.6Kbps FAX/ Modem, MVPV34i 16-bit ISA card, 33.6Kbps Data, 14.4Kbps FAX, RJ-45, w/ Software OR Action Tec 33.6 Fax/Modem, ACTISA336(USA)	108.12
0017AB	SMC EtherEZ NIC, 8416BTA 16-bit ISA, RJ-45/BNC/AUI Connections w/ “T” Connector & Software	48.96

CLIN	DESCRIPTION	PRICE
	OR 3COM	
0017AC	RAYLAN, FIBER OPTIC NIC, 1000-10-NIC 16-bit ISA, ST & RJ-45 Connectors, 10BaseFL & 10baseT, w/ Software	127.50
0017AE	TRACKBALL PRO, CH PRODUCTS, 400-501 Serial Trackball, Version 1.0, 2.25" Diameter Ball	86.70
0017AF	U.K. MODEM MultiTech, MultiModem LT, MT1432LTI-UK, PCMCIA Card, HNA/CA for UK, 14.4bps Data/FAX Modem w/ Software	255.00
0017AG	JAPAN MODEM MultiTech, MultiModem PC, MT1432BCI-Japan 16-bit ISA, HNA/CA for Japan, 14.4bps Data/FAX Modem w/ Software	255.00
0017AH	ITALY MODEM MultiTech, MultiModem LT, MT1432LTI-Italy PCMCIA Card, HNA/CA for Italy, 14.4bps Data/FAX Modem w/ Software	255.00
0017AJ	PCMCIA ETHERNET CARD ActionTec, Ethernet PCMCIA NIC, PE-200C, 10Base2 & 10BaseT, w/ RJ-45 & BNC Connectors and Software	71.40
0017AK	INTEL ETHEREXPRESS PRO/100 OR 3COM ETHERLINK XL, 3C905-TX 10/100 Base TX PCI Adapter	109.14
0017AL	SMC ETHERPOWER ETHERNET PCI COMBO ADAPTER SMC8432BTA OR 3COM ETHERLINK XL ETHERNET COMBO ADAPTER, 3C900-COMBO	100.98
0017AM	PCI ULTRA SCSI CONTROLLER, ADAPTEC, AHA-2940US	185.64
0017AN	ISA SCSI CONTROLLER, ADAPTEC, AHA-1542CP	227.46
0017AP	SCSI PCMCIA CARD, ADAPTEC, APA 1460A-2	173.40
0017AQ	ACTION TEC PCMCIA CARD READER, REAR LOAD, PER-01083-0000	47.94
0017AR	ACTION TEC PCMCIA CARD READER, FRONT LOAD, PER-0396A-0000	67.32
0017AS	ADAPTEC PCI TO ULTRA WIDE CONTROLLER KIT, AHA2940UW	282.54
0017AT	ADAPTEC TOTAL CD 16bit ISA CONTROLLER KIT, AVA1505VK	55.08
0017AU	BOCA 33.6 EXTERNAL DATA/FAX MODEM, MV34ED	81.60
0018AA	16-BIT STEREO SOUND CARD W/ 2 SPEAKERS AND AUDIO VISUAL SW Sound Card: Creative Labs, 20299291001 OR Ensoniq, 9923001701 w/stereo speakers & software, LCS-1020	91.80
0019AA	CONUS SURGE SUPPRESSOR, EFI ELECTRONICS, MPS-6 Navy Surge and Noise Protector, 50-400Hz, 90-130VAC, 6 Outlets, 15 Amp, RFI/EMI,	59.16

CLIN	DESCRIPTION	PRICE
	Metal Case, 6' Cord	
0019AD	CANON NOTEBOOK PRINTER BATTERY, NiMH, NB-300 for CLIN 0016AB CANON BJ-30	76.50
0019AE	OCONUS POWER ADAPTER KIT, LEE TECH, IEC320 C13+3221UK/6071T/1400JK	30.60
0019AG	BACK-UPS PRO 280 VA UPS w\ PowerChute SW, APC BP280BPNP	139.74
0019AH	BACK-UPS PRO 280 VA UPS INTL 230v w\ PowerChute SW, APC BP280BIPNP	160.14
0019AJ	SMART-UPS v\s 420 VA w\ PowerChute SW, APC SUVS420	224.40
0019AK	SMART-UPS v\s 420 VA INTL, (230v) w\ PowerChute SW, APC SUVS420I	234.60
0019AL	SMART-UPS 700 VA, APC SU700NET, w\ PowerChute SW for Novell and NT	371.28
0019AM	SMART-UPS 700 VA INTL, (230v) w\ PowerChute SW for Novell and NT, APC SU700INET	385.56
0019AN	SMART-UPS 2200 VA UPS, APC SU2200X93 *see Footnote 1	1,107.72
0019AP	SMART-UPS 450 VA UPS, APC SU450X93 *see Footnote 1	390.66
0019AQ	SMART-UPS 700 VA UPS, APC SU700X93 *see Footnote 1	461.04
0019AR	SMART-UPS 1000 VA UPS, APC SU1000X93 *see Footnote 1	592.62
0019AS	SMART-UPS 1400 VA RACKMOUNTED UPS, APC SU1400RMX93 *see Footnote 1	831.30
0019AT	LITHIUM ION BATTERY - for STEPNOTE 5 (CLINS 0005AL-5AT)	160.14
0019AU	APC SMART UPS 1400, SU-1400 NET	608.94
0019AV	APC SMART UPS 1000, SU-1000 NET	499.80
0019AW	STEPNOTE SC NIMH BATTERY, KIT-0368-SC00	99.96
0019AX	STEPNOTE SC LITHIUM BATTERY, KIT-0368-SC01	173.40
0019AY	LITHIUM BATTERY UPGRADE STEPNOTE SC Note: This upgrade must be purchased at time of order	81.60
0041CD	MICROSOFT WINDOWS 95 (CD-ROM MEDIA)	80.58
0041FD	MICROSOFT WINDOWS 95 (FLOPPY DISK MEDIA)	80.58
0042FD	CENTRAL POINT, PC TOOLS PRO V9.0-DOS (FLOPPY DISK MEDIA)	15.30
0043FD	CENTRAL POINT, PC TOOLS PRO V2.0-WIN (FLOPPY DISK MEDIA)	25.50
0044FD	ELIASHIM MICROCOMPUTER, VIRUSAFE & MASTERSAFE FOR WINDOWS 95 (FLOPPY DISK MEDIA)	30.60
0045FD	MICROSOFT TCP/IP-32 for WFW 3.11 (FLOPPY DISK MEDIA) 32-bit TCP/IP Support, WFW Provides Peer-to-Peer Support	5.10
0046CD	LOTUS SMARTSUITE 4.0: Lotus 1-2-3, Word Pro, Approach, Freelance Graphics and Lotus Organizer (CD-ROM MEDIA)	40.80
0046FD	LOTUS SMART SUITE 4.0: Lotus 1-2-3, Word Pro, Approach, Freelance Graphics and Lotus Organizer (FLOPPY DISK MEDIA)	40.80
0047CD	MICROSOFT OFFICE PROFESSIONAL V4.3 w/ BOOKSHELF, 269-054V4VL Office, Word, Excel, PowerPoint and Access. (CD-ROM MEDIA)	157.08
0047FD	MICROSOFT OFFICE PROFESSIONAL V4.3 w/ BOOKSHELF, 269-054V4VL Office, Word, Excel, PowerPoint and Access. (FLOPPY DISK MEDIA)	173.40
0048CD	MICROSOFT OFFICE PROFESSIONAL V7.0, 269-7054V700 Office, Word, Excel, PowerPoint, Access and Schedule+. For use with Windows 95 and Windows NT, (CD-ROM MEDIA)	357.00
0048FD	MICROSOFT OFFICE PROFESSIONAL V7.0, 269-7054V700 Office, Word, Excel, PowerPoint, Access and Schedule+. For use with Windows 95 and Windows NT, (FLOPPY DISK MEDIA)	393.72
0049CD	MICROSOFT WINDOWS NT WORKSTATION (CD-ROM MEDIA)	260.10
0050CD	MICROSOFT WINDOWS NT WORKSTATION UPGRADE FACTORY INSTALLED: This CLIN can only be ordered when ordering a desktop or notebook system. This is an upgrade from Windows 95 to Windows NT Workstation. (CD-ROM MEDIA)	119.34
0052FD	MS WINDOWS FOR WORKGROUPS 3.11, FACTORY INSTALL (FLOPPY DISK MEDIA) This CLIN can only be ordered when ordering a desktop or notebook system.	NSP
0060AA	Product Solutions (ODCs)	TBD

Footnote 1: Per NAVY Message 211354Z NOV 94 FM COMNAVAIRLANT NORFOLK VA
Subject: Uninterruptible power Supplies for personal computers (UPS)

UPS X93 models permanently affixed with a nameplate verifying it as an X93 model should be considered to be compatible with shipboard power systems.

NCTAMS LANT Points of Contact
Technical Specifications and Support Branch

Ordering: Diane White
Phone: (757) 445-1493; DSN 565
E-mail : diane_white@ccmail.nctamslant.navy.mil
Tech Support: Sandy Mieczkowski (757) 445-2568; DSN 565
E-mail : sandy_mieczkowski@ccmail.nctamslant.navy.mil